

PaperVision® Enterprise Administration and Architecture Guide

Version 85.0



Information in this document is subject to change without notice and does not represent a commitment on the part of Digitech Systems, LLC. The software described in this document is furnished under a license agreement or nondisclosure agreement. The software may be used or copied only in accordance with the terms of the agreement. It is against the law to copy the software on any medium except as specifically allowed in the license or nondisclosure agreement. No part of this manual may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, for any purpose without the express written permission of Digitech Systems, LLC.

Copyright © 1997–2019 Digitech Systems, LLC. All rights reserved.

Printed in the United States of America.

PaperVision, the PaperVision logomark and ImageSilo are registered trademarks of Digitech Systems, LLC.

PaperFlow is a trademark of Digitech Systems, LLC.

Microsoft, Windows, SQL Server, Access, and .NET Framework are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

All other trademarks and registered trademarks are the property of their respective owners. The Microsoft Office User Interface is subject to protection under U.S. and international intellectual property laws and is used by Digitech Systems, LLC under license from Microsoft.

PaperVision Enterprise contains text search technology provided under license by dtSearch®. All rights reserved.

PaperVision Enterprise contains technology under license from Autonomy, Inc. All rights reserved.

PaperVision Enterprise contains portions of imaging code owned and copyrighted by Pegasus Imaging Corporation, DBA Accusoft Pegasus, Tampa, FL. All rights reserved.

PaperVision Enterprise contains portions of code owned and copyrighted by Aspose Pty Ltd. All rights reserved.



Digitech Systems, LLC
8400 E. Crescent Parkway, Suite 500
Greenwood Village, CO 80111
Phone (303) 493-6900
Toll Free (866) 374-3569
www.digitechsystems.com

CONTENTS

CHAPTER 1 Introduction

Welcome	18
Licensing Information	18
System Requirements	19
Minimum Software Requirements	19
Minimum Hardware Requirements	20
Terms You Should Know	21
Administrators	21
Data Group	21
Documents	22
Detail Sets	22
Entity	22
Entity ID	23
Index Values	23
Project	23
Date and Time Format Information	23
Get Product Support	24
Administration Console Access	24
To log in to the Administration Console	24
To log out of the Administration Console	24

CHAPTER 2 Global Administration

Global Administration Overview	26
To access global administration settings	26
Automation Service Status Tasks	26
To determine which automated processes are running	26
To start an automation server process	27
To stop an automation server process	27
To delete an automation server process	27
To refresh an automation server process	27
Configure Multiple Automation Service Processes	28
To change the number of simultaneous processes	28
Deletion Queue	29
To view the Deletion Queue	29
To refresh the Deletion Queue	29
To delete items from the Deletion Queue	29
To manually process an item in the Deletion Queue	29
Email Queue	30
To view the Email Queue	30
To view the properties of an item in the Email Queue	30
To delete items from the Email Queue	30
To refresh the Email Queue	31
Global Administrators	31
To view global administrators	31
To create a new global administrator	31
To refresh the Global Administrators list	32
To set a password for a global administrator	32
To delete a global administrator	33
To edit properties of a global administrator	33
Import	33



To access import functions	33
Import Queue	34
To view the Import Queue	34
To view the properties of an item in the Import Queue	34
To refresh the Import Queue	35
To delete an item from the Import Queue	35
To enable an item on the Import Queue	35
To disable an item on the Import Queue	35
Monitored Import Paths	36
To view monitored import paths	37
To create a monitored import path	37
To refresh monitored import paths	37
To delete a monitored import path	38
To modify multiple monitored import paths	38
To modify the properties of a monitored import path	38
Import Logs	39
To view Import Logs	39
To delete log entries for a date range	39
To export log entries for a date range to an XML file	39
To archive log entries	40
To view import log archives	40
To refresh the Import Logs	40
To delete log entries	41
To export log entries to an XML file	41
To view the properties of a log entry	41
Licensing	42
To view existing licenses	42
To add a new license	42
To bulk import licenses	43
To refresh the list of licenses	43
To delete a license	44
To view license properties	44
Maintenance	44
To access maintenance functions	44
Maintenance Queue	44
To view the Maintenance Queue	45
To refresh the Maintenance Queue	45
To delete items from the Maintenance Queue	45
To view the properties of an item on the Maintenance Queue	45
Maintenance Logs	46
To view the Maintenance Logs	46
To refresh the Maintenance Logs	46
To delete log entries	46
To export log entries to an XML file	46
To view the properties of a log entry	47
Migration Jobs	47
Notifications at the Global Level	47
To view notifications	47
To create a new notification	48
To refresh the list of notifications	48
To delete an item from the list of notifications	48
To view the properties of a notification	48
Process Locks	49
To view process locks	49
To refresh the list of process locks	49
To delete a process lock	49
Report Management Errors	50

System Settings	50
To access system settings functions	50
Configure System Settings	50
To access system settings	50
General System Settings	51
To set utilization limits	51
To set options for server-side processing	51
To set the maximum number of display items for reports/notifications	52
To set the server-side encryption key	52
To set the client ping increment	52
Data System Settings	53
To set data processing items	53
To set options for data size management	54
To set options for Report Management	55
To set options for log archiving	55
Replication System Settings	56
Replication Destination Paths	56
To add replication destination paths	57
To delete replication destination paths	57
Replication Journal Entry Paths	57
To add replication journal entry paths	57
To edit a replication journal entry path	58
To delete replication journal entry paths	58
Email and Notifications System Settings	58
To configure email settings	58
To set the notification method for the global administrator	59
Local System Settings	60
To configure local settings	60
To configure automation service logging	61
Configure Automation Service Scheduling	61
Available Operations	61
To open the Automation Service Schedule	63
To add an automation service operation	63
To edit an automation service operation	64
To change the evaluation order for an automation service operation	64
To remove an automation service operation	65
View Full-Text Queue Statistics	65
To view full-text queue statistics	65
 CHAPTER 3 Entity Configuration	
Entity Configuration Tasks	68
To view existing entities	68
To add a new entity	68
To change data group paths for all entities	69
To find an entity ID	69
To refresh the list of entities	70
To delete an entity	70
To set entity properties	70
To complete orphaned worksteps	71
To verify/create database indexes	71
 CHAPTER 4 Entity Administration	
Setting Entity Properties	74
To access entity properties	74
General Entity Properties	74
To set the entity name	74
To set database properties	74
To set entity paths	75

To set migration job properties	76
To disable the entity	77
To disable utilization tracking	77
Contacts and Notification Entity Properties	78
To add a technical contact	78
To add a billing contact	78
To set the notification method for users	78
Import Entity Properties	79
To set the default import data group state	79
To load COLD data and external documents into the full-text database	79
To keep data group database archives after import	80
To set the default import type	80
To set import error handling	81
To apply object changes during reload	82
To set the default import copy settings	82
To send email validation reports after import	83
To set data group auto-mapping	83
Display Entity Properties	84
To set the default character case display	84
To set the default document grouping	84
To set the default web document display method	85
To display a notification when an upgraded document viewer is available	85
To set file types to display in registered application	86
To set utilization report options	86
Backup Processing	87
To access backup processing options	87
Backup Jobs	88
To view backup jobs	88
To add a backup job	88
To refresh the list of backup jobs	89
To delete backup jobs	89
To edit the properties of a backup job	90
Processing Logs	90
To view the Processing Logs	90
To refresh the Processing Logs	90
Current Activity	91
To access current activity options	91
Current Sessions	91
To view the current user sessions	92
To kill current user sessions	93
To refresh the list of current user sessions	93
Document Grants	93
To view the active document grants	93
To delete document grants	94
To refresh the list of active document grants	94
Locked Users	94
To view locked users	94
To unlock a locked user	94
To refresh the list of locked users	95
Notifications at the Entity Level	95
To view entity notifications	95
To create a new notification	96
To refresh the list of notifications	96
To delete notifications	96
To view the properties of a notification	96
Data Storage	97
To access data storage options	97
Data Groups	97

To access data group functions	97
Filter the Data Groups List	99
To filter the data groups list	99
To remove a filter from the data groups list	99
Refresh the Data Groups List	100
To refresh the data groups list	100
Print the Data Groups List	100
To print the data groups list	100
Create New Attachment Data Groups	101
To create a new attachment data group	101
Import Data Groups	101
To import a data group	102
Data Group Types for Import	105
About C.A.R. Data Groups	105
About XML Data Groups	106
PaperVision Package Files	106
Modify Data Group Paths	108
To modify data group paths	108
Resize Data Groups	108
To resize data groups	108
Move Data Groups	109
To move data groups	110
Encrypt and Decrypt Data Groups	110
To submit data groups for encryption	111
To submit data groups for decryption	111
Migrate Data Groups	112
To migrate data groups	112
Back Up Data Groups	112
To back up data groups	112
Validate Data Groups	113
To submit selected data groups for validation	113
To submit all listed data groups for validation	114
Change the Read/Write State for All Data Groups	114
To change the Read/Write state for all listed data groups	114
Empty Data Groups from the Recycle Bin	115
To empty data groups from the Recycle Bin	116
Restore Data Groups from the Recycle Bin	116
To restore data groups from the Recycle Bin	116
Purge Data Groups	117
To purge data groups	118
Edit Data Group Properties	118
To edit data group properties	119
Message Capture File Sets	119
To access functions for Message Capture File Sets	119
Filter the Message Capture File Sets List	121
To filter the Message Capture File Sets list	121
To remove a filter from the Message Capture File Sets list	121
Refresh the Message Capture File Sets List	122
To refresh the Message Capture File Sets list	122
Print the Message Capture File Sets List	122
To print the Message Capture File Sets list	122
Roll Back Message Capture File Sets	123
To roll back Message Capture File Sets	123
Export Message Capture File Sets	124
To export Message Capture File Sets	124
Empty Message Capture File Sets from the Recycle Bin	124
To empty Message Capture File Sets from the Recycle Bin	125
Restore Message Capture File Sets from the Recycle Bin	125

To restore Message Capture File Sets from the Recycle Bin	126
View Message Capture File Sets Properties	126
To view properties for Message Capture File Sets	126
Report Management File Sets	127
To access functions for Report Management File Sets	127
Filter the Report Management File Sets List	129
To filter the Report Management File Sets list	129
To remove a filter from the Report Management File Sets list	129
Refresh the Report Management File Sets List	130
To refresh the Report Management File Sets list	130
Print the Report Management File Sets List	130
To print the Report Management File Sets list	130
Roll Back Report Management File Sets	131
To roll back Report Management File Sets	131
Export Report Management File Sets	132
To export Report Management File Sets	132
Empty Report Management File Sets from the Recycle Bin	132
To empty Report Management File Sets from the Recycle Bin	133
Restore Report Management File Sets from the Recycle Bin	133
To restore Report Management File Sets from the Recycle Bin	133
View Report Management File Sets Properties	134
To view properties for Report Management File Sets	134
General Security	135
To access general security options	135
Encryption Keys	135
To add an encryption key	136
To refresh the encryption key list	136
To delete encryption keys	136
To edit encryption key properties	137
Security Policy	137
To access security policies configuration	137
General Security Policy	138
To set general security options	138
To set the maximum session idle time	138
To assign encryption keys	139
To set the pass phrase for inter-process communications	139
Account Lockout Security Policy	140
To set the maximum session idle time	140
Authentication Security Policy	140
To set login restrictions	141
To assign an encryption key to the remote authentication gateway	141
Passwords Security Policy	141
To set password options	141
System Groups	142
To view system groups	142
To add a system group	142
To refresh the system groups list	143
To delete system groups	143
To edit system group properties	143
System Users	144
To view system users	144
To add a system user	144
To import users	146
To refresh the system users list	146
To set a user password	146
To delete system users	147
To edit system user properties	147
File Format for Importing Users	148

Migration Jobs	149
Migration Job Configuration Options	149
Status and Tasks for Submitted Migration Jobs	150
To view the status of migration jobs	150
To refresh the list of migration jobs	151
To cancel a migration job	151
To view properties for a migration job	151
To resubmit a user list or data group migration job	152
To copy a project migration job	152
To edit a project migration job	153
CHAPTER 5 Project Configuration	
Project Configuration Overview	156
To access project configuration functions	156
Add Projects	157
To add a project	157
Refresh the Projects List	158
To refresh the projects list	158
Delete Projects	158
To delete projects	158
Empty the Recycle Bin	158
To empty the Recycle Bin	158
Submit Projects for Full-Text Rebuild	159
To submit projects for full-text rebuild	159
Submit Projects for Full-Text Recreation	159
To submit projects for full-text recreation	159
Submit Projects for Full-Text Compression	160
To submit projects for full-text compression	160
Submit Projects for Version Cleanup	160
To submit projects for version cleanup	160
Submit Projects for Migration	161
To submit projects for migration	161
Edit Project Properties	162
To edit project properties	162
Configure Index Fields	163
To add document index fields	163
To edit document index fields	167
To delete document index fields	167
To add Message Capture index fields	167
To reorder document index fields	168
CHAPTER 6 Project Administration	
Enhanced Auditing	170
To configure enhanced auditing for a project	170
Disclosure Reason List	171
To configure disclosure reasons	171
Disclosure Recipient List	172
To configure disclosure recipients	172
Document Associations	172
To access document association functions	173
Add Document Associations	173
To add document associations	174
Import Document Associations	175
To import document associations	175
Refresh the Document Associations List	175
To refresh the document associations list	175

Delete Document Associations	175
To delete document associations	175
Export Document Associations	176
To export document associations	176
Edit Document Association Properties	176
To edit document association properties	176
Document Security Levels	177
To access document security levels functions	177
Add Document Security Levels	177
To add document security levels	178
Refresh the Document Security Levels List	179
To refresh the document security levels list	179
Apply Document Security Levels to Current Documents	180
To apply document security levels to current documents	180
Submit Document Security Levels to be Applied to Current Documents	180
To submit document security levels to be applied to current documents	180
Delete Document Security Levels	181
To delete document security levels	181
Edit Properties for Document Security Levels	181
To edit properties for document security levels	181
Integration Definitions	182
Important Prerequisites	182
To access functions for integration definitions	182
Add Integration Definitions	183
To add integration definitions	183
Import Integration Definitions	186
To import integration definitions	186
Refresh the Integration Definitions List	186
To refresh the integration definitions list	186
Delete Integration Definitions	187
To delete integration definitions	187
Export Integration Definitions	187
To export integration definitions	187
Edit Properties for Integration Definitions	188
To edit properties for integration definitions	188
Security Access	188
To access security access functions	188
Add Project Security Access	188
To add new project security access	189
Refresh the Security Access List	191
To refresh the security access list	191
Delete Security Access	192
To delete security access	192
Edit Properties for Security Access	192
To edit properties for security access	192
Directory Manager Jobs	193
To view directory manager jobs	193
To add directory manager jobs	193
To refresh the directory manager jobs list	196
To delete directory manager jobs	196
To edit properties for directory manager jobs	196
About Directory Manager Jobs and PaperVision Package Files	197
Records Destruction Lists	198
To view records destruction lists	198
To clean up records destruction lists	199
To refresh the records destruction list	199
To delete records destruction lists	199

Records Retention Policy Sets	200
To view records retention policy sets	200
To import records retention policy sets	201
To refresh the records retention policy sets list	201
To delete records retention policy sets	201
To export records retention policy sets to an XML file	202
To edit properties for records retention policy sets	202
To clear document destruction or lock information	203
Add Records Retention Policy Sets	204
To add records retention policy sets	205
 CHAPTER 7 Message Manager	
Message Manager Overview	210
Message Capture File Sets Overview	210
Non-Repudiation Process	211
Document Indexing	211
Message Capture Policy Sets	212
To view Message Capture Policy Sets	212
To import Message Capture Policy Sets	212
To refresh the Message Capture Policy Sets list	213
To delete Message Capture Policy Sets	213
To export Message Capture Policy Sets to an XML file	213
To edit properties for Message Capture Policy Sets	214
Add Message Capture Policies	214
To specify general options	215
To add policies	215
To specify file set options	215
General Settings	216
To set the general options for a Message Capture Policy	216
Message Settings	217
To set the message options for a Message Capture Policy	217
Sender Settings	219
To set sender addresses for a Message Capture Policy	219
To set sender active directory group names for a Message Capture Policy	219
Recipient Settings	220
To set recipient addresses for a Message Capture Policy	220
To set recipient active directory group names for a Message Capture Policy	221
 CHAPTER 8 Report Management	
Report Management Overview	224
Report Management File Sets Overview	224
Report Management Jobs	225
To view Report Management Jobs	225
To import Report Management Jobs	226
To refresh the Report Management Jobs list	226
To delete Report Management Jobs	226
To export Report Management Jobs to an XML file	227
To edit properties for Report Management Jobs	227
To deactivate or activate Report Management Jobs	228
Add Report Management Jobs	228
To add Report Management Jobs	228
General Settings	229
To set general options for a Report Management Job	229
File Settings	230
To set file options for a Report Management Job	230
To configure character replacement options	231
To configure text sequence removal options	232

Line Settings	232
To set line options for a Report Management Job	232
Page Settings	233
To set page options for a Report Management Job	233
To configure text sequence removal options	235
Page Detection Methods	236
Configure Text Sequences	236
To configure text sequences	236
Configure Custom Control Codes	237
To configure custom control codes	237
Configure ASA/ANSI with Channel Commands	238
To configure ASA/ANSI with channel commands	239
Configure AS400 Spool	240
To configure AS400 spool codes	240
Fields and Breaks Settings	241
To set fields/breaks options for a Report Management Job	241
Configure Fields and Breaks	242
To access fields and breaks configuration options	242
To configure regions	243
To configure fields	245
Document Indexing Terms and Concepts	246
Regions	246
Normal Regions	246
Detail Regions	247
Anchors	247
Fixed Anchors	247
Floating Anchors	247
Fields	247
Test Execution	247
To run a test and access results	248
Form Overlay Settings	249
To configure form overlays for a Report Management Job	249
Setup Overlay	250
To access setup overlay options	250
To set overlay text display properties	251
To modify the overlay form	252
Report Management Parsing Engine Overview	253
Report Management Errors	254
To view Report Management Errors	254
To delete Report Management Errors for a date range	254
To export Report Management Errors for a date range to an XML file	255
To refresh the list of Report Management Errors	255
To delete Report Management Errors	255
To export Report Management Errors to an XML file	256
To view the properties of a Report Management Errors	256

CHAPTER 9 WorkFlow

WorkFlow Overview	258
Terms You Should Know	258
Workflow	258
Workflow Definition	259
Workflow Instance	259
Pre-Conditions	259
Workstep Definition	259
Workstep Instance	259
Workstep Owner	259
Workstep Participant	260
Task	260

Workstep Transition	260
Post-Condition	260
Plan Your Workflow	260
Worksteps vs Tasks	261
Worksteps Overview	261
Automated Worksteps	261
Manual Worksteps	262
Custom Code Worksteps	262
WorkFlow Custom Code Server	262
To download the PaperVision Custom Code Server	263
To change the WorkFlow Initiator Service interval	263
WorkFlow Custom Code Server Configuration Tool	264
To specify the number of processes running on the WorkFlow Custom Code Server	264
To specify the worksteps processed by a worker instance	264
To copy a worker instance	265
To view the WorkFlow Custom Code Server status	265
WorkFlow Definitions	266
To view workflow definitions	266
To add a new workflow definition	266
To refresh the list of workflow definitions	266
To delete workflow definitions	267
To edit the properties of a workflow definition	267
Configure Workflow Definitions	268
To open the WorkFlow Designer	268
To configure a workflow definition	269
To add a pre-condition to a workflow definition	269
To import a workflow definition	271
To export a workflow definition	271
Add Worksteps	272
To add an automated workstep	272
To add a custom code workstep	273
To add a manual workstep	274
Link Worksteps	275
To link worksteps on the Layout tab	275
Custom Code Worksteps	276
To add a Transition to a custom code workstep	277
Add Tasks	277
To add a task	277
Add Post-Conditions	279
To add a post-condition to an automated workstep	279
To add a post-condition to a manual workstep	282
Verify Workflows	283
To verify a workflow definition	283
WorkFlow Verification Results	284
WorkFlow Verification Checks	286
Viewing Workflow Definition Diagrams	287
To view a workflow definition diagram	287
Activate and Deactivate a Workflow Definition	288
To deactivate and activate a workflow definition	288
Configure Email Messages	288
To configure an email message	288
Email Message Tags	290
CURRENTDATETIME Tags	293
CHAPTER 10 Reports	
Report Functions	296
To access reports	296

To apply or remove a report filter	296
To refresh reports	297
To print reports	297
To export report data to an XML file	297
Report Archives	297
To view report archives	298
To archive reports	298
To restore report archives	298
Document Access	299
Records Retention/Destruction	299
To access the Records Retention/Destruction report	300
To view document lock and destruction information	300
To navigate through documents	301
System Operations/Queries	301
Utilization	302
To access the Utilization report	303
Workflow History	303
To view the Workflow history of a Workflow instance	304
Workflow Status	304
To view the Workflow status of a Workflow instance	305
Move Workflow Instances to a Specific Workstep	305
To move Workflow instances to a specific workstep	305

APPENDIX A System Architecture

SQL Server Express Edition	308
Web vs. Application Servers	308
Web Services	309
No IIS Sessions Required	309
Load Balancing	310
Automation Service and Servers	310
Database Scaling	311
File Replication	312
System Design Scenarios Overview	312
Single User	312
Workgroup	313
Department	314
Large Enterprise	315
Security Features Overview	316
Session ID Encryption	316
Support for SSL and Non-Standard Ports	316
Function-Level Verification	316
Session Source Persistence	316
IP Address Limiting	317
Automatic Session Termination	317
Data Segregation	317
Data Encryption	317

APPENDIX B Various Configuration Items

Set Up Process Redirection	320
Setup Assumptions	320
Configuring a Web Server to Use a Separate Application Server	321
Process Redirection with the PaperVision Document Search Service	321
To set up a web server not using SSL to redirect to a web/application server not using SSL	321
To set up a web server not using SSL to redirect to a web/application server using SSL	322
To set up a web server using SSL to redirect to a web/application server not using SSL	323

To set up a web server using SSL to redirect to a web/application server using SSL	324
To set up an application server at the end of a redirect	325
Process Redirection with the PaperVision File Service	326
To set up a web server not using SSL to redirect to a web/application server not using SSL	326
To set up a web server not using SSL to redirect to a web/application server using SSL	327
To set up a web server using SSL to redirect to a web/application server not using SSL	327
To set up a web server using SSL to redirect to a web/application server using SSL	328
To set up an application server at the end of a redirect	329
Configure Document Search Service for SSL	329
To use the PaperVision Document Search Service with SSL	329
Document Search Service Performance Counters	330
Configure File Service for SSL	330
To use the PaperVision File Service with SSL	330
Set Custom Font and Colors	331
Customization Options	331
PaperVision Enterprise APIs	332
PaperVision Enterprise Web and ASPX Pages	332
PVESearchURL.aspx Page	333
PVESystemHealth.ASPX Page	333
APPENDIX C Remote Authentication	
Remote Authentication Functional Overview	336
Remote Authentication Use Scenarios	336
PaperVision Repository within the Same Active Directory Domain	336
ImageSilo or PaperVision Repository within a Different Active Directory Domain	337
Configure PaperVision Authentication Gateway Settings	338
To log in to the PaperVision Enterprise Administration Console	338
To create a PaperVision Enterprise user	338
To create an encryption key	340
To assign the encryption key to the entity security policy	340
To configure PaperVision Gateway Settings	340
Accessing the Authentication Gateway	341
To access the Authentication Gateway	341
Using PaperVision Search URL to Access the Authentication Gateway	341
Using PaperVision Tools to Access the Authentication Gateway	341
To configure the Authentication Gateway in PaperVision Tools	341
APPENDIX D Search Assistance	
Search Process Overview	344
Search Process for Documents (Excluding Full-Text Search Criteria)	344
Search Process for Documents (Including Full-Text Search Criteria)	345
Search Criteria Guidelines	346
Regular Expression Syntax and Metacharacters	348
APPENDIX E Utilities	
PaperVision Enterprise Configuration Utility Overview	354
To open the PaperVision Enterprise Configuration Utility	354
Change the Number of Simultaneous Processes	355
To change the number of simultaneous processes	355
Change SQL Server Connection Information	356
To change SQL server connection information	356
Digitech Logging Utility Overview	357
Configure Listeners	357
To configure the Windows Event Log Listener	357
To configure the Email Listener	358
To configure the File Listener	358

To configure the Rolling File Listener	360
Configure the Digitech Logging Utility	362
To configure the Digitech Logging Utility	362

CHAPTER 1

Introduction

Welcome	18
Licensing Information	18
System Requirements	19
Terms You Should Know	21
Date and Time Format Information	23
Get Product Support	24
Administration Console Access	24



Welcome

PaperVision Enterprise provides the ability to securely store and retrieve any type of corporate information and manage its flow within your organization. This product provides full features and functionality with unparalleled scalability, reliability, and security. The Administration Console provides you with access to all administrative functions, and this documentation will guide you through the available features and how to use them. You can also see "Get Product Support" on page 24 for resources where you can learn more about our products. Before you begin working in PaperVision Enterprise, reviewing the content under "Terms You Should Know" on page 21 will help you use the product and its documentation more effectively. When you are ready to begin, go to "Administration Console Access" on page 24 for step-by-step instructions to access the Administration Console.

Licensing Information

As stated in your End-User License Agreement (EULA), PaperVision Enterprise is licensed per-concurrent user. This provides the greatest flexibility in licensing, as a license is used only when a user is logged into the system (no licenses are used for administration). If all of the licenses are in use, the user is prompted that there are no licenses available for their session. If you are hosting PaperVision Enterprise for multiple entities (such as in an on-demand model), keep in mind that concurrent licenses (either individual, in groups, or unlimited) are assigned to a specific entity.

- **PaperVision® Enterprise WorkFlow** is licensed on a per-entity basis. An unlimited license allows an unlimited number of users for a single entity (of course, still limited to the number of concurrent PaperVision licenses) to access WorkFlow functionality. If concurrent WorkFlow licenses are purchased, any user who logs into PaperVision Enterprise who has access to WorkFlow functionality (that is, they are a member of a group that is a WorkFlow participant) is required to have a WorkFlow license and a PaperVision license available to log in.
- **PaperVision® Enterprise Report Management** is licensed on a per-entity basis. This allows an unlimited number of Report Management Jobs to be defined and processed for a single entity.
- **PaperVision® Tools** is licensed as a component of PaperVision Enterprise. PaperVision Tools is a suite of tools which integrate PaperVision functionality into third-party applications. Users with current PaperVision Enterprise maintenance contracts can install and use PaperVision Tools.
- **PaperVision® Message Manager** is comprised of the PaperVision Message Capture Server and PaperVision Message Capture Harvester components. PaperVision Message Manager is an included component of PaperVision Enterprise.
- Web servers, application servers, and automation servers are all included with the standard PaperVision Enterprise concurrent licenses. You can install an unlimited number of these servers, for even a single concurrent license.

See "Licensing" on page 42 for information about licensing tasks that global administrators can perform.

System Requirements

This content describes the minimum software and hardware requirements for PaperVision Enterprise.

Minimum Software Requirements

The following table shows the minimum system requirements for PaperVision Enterprise and its optional components.

Software	Version
Operating Systems	<p>Windows® 2008 R2, 2012, 2012 R2, or 2016 is required for servers running PaperVision Enterprise server.</p> <p>Windows 7, 8, 8.1, or 10 is required for the following components:</p> <ul style="list-style-type: none"> ■ PaperVision Administration Console ■ PaperVision Assistant ■ PaperVision Automation Service (optional) <p>Including all latest versions of the OS with all required (not optional) Windows updates</p> <p>PaperVision Web/Application or Authentication Gateway Server (optional) both require Internet Information Server (IIS) 7.5 or later.</p>
Microsoft® .NET Framework	Version 4.5 or later
Windows PowerShell	Version 1.0 or later
Microsoft® SQL Server	<p>SQL Server 2008 or later</p> <p>NOTE: Optionally, you can install Microsoft SQL Server Express Edition. We support SQL Server Express 2008 R2 or later.</p>
Internet Browser	<p>Internet Explorer® 11 (PaperVision Viewer and Browser-Based Viewer)</p> <p>Mozilla Firefox® latest version (PaperVision Viewer and Browser-Based Viewer)</p> <p>Google Chrome™ latest version (PaperVision Viewer and Browser-Based Viewer)</p> <p>Safari® on iPad devices and Macs latest version (Browser-Based Viewer)</p>

Minimum Hardware Requirements

Most enterprise software is capable of operating on a basic hardware configuration that includes a current processor and 4 GB of memory for desktops and 8 GB of memory for servers. However, each organization and their intended use of PaperVision Enterprise are unique. The intended workload, (including the maximum number of users, and the quantity and types of operations performed within a specific periodicity, etc.) coupled with security and redundancy requirements will dictate the hardware requirements for each implementation.

PaperVision Enterprise has the distinct capability to scale both up and out. You can configure most of the functions performed by PaperVision Enterprise to take advantage of powerful hardware configurations, such as those with many processor cores and hundreds of GB of memory (scaling up). Additionally, PaperVision Enterprise can spread its processing requirements across numerous computers (scaling out).

PaperVision Enterprise products are designed and tested for specific operating systems, not hardware environments. Numerous customers successfully run PaperVision Enterprise in virtual environments, including VMware® and Microsoft® Hyper-V. While this technology has matured over the years, issues have occurred with common software (other than PaperVision Enterprise) not operating properly or efficiently because of the virtual environment. In the cases that Digitech Systems' Technical Support has witnessed, the issue was with the virtual environment, not our software.

If our technical support believes that the hardware environment (including virtual environments) is contributing to an operational or performance issue, they may request that you ensure the issue exists in a different (or non-virtual) environment.

If you intend to use a virtual environment for your PaperVision Enterprise implementation, carefully consider the implications of running in a shared environment. Remember, you are not just sharing processors and memory. You are also sharing network and disk resources with the other virtual environments on the same hardware.

Component	Requirement
Hard Disk Space	1.05 GB (installation only)
Screen Resolution	SVGA Monitor (1024 x 768 or higher recommended)

Terms You Should Know

This content contains definitions for terms that are used throughout the documentation and online help. Knowing this terminology will help you use the product and its documentation more effectively.

- See "Administrators" below for a definition of the types of administrators.
- See "Data Group" below for a definition of this term.
- See "Documents" on the next page for a definition of this term.
- See "Detail Sets" on the next page for a definition of this term.
- See "Entity" on the next page for a definition of this term.
- See "Entity ID" on page 23 for a definition of this term.
- See "Index Values" on page 23 for a definition of this term.
- See "Project" on page 23 for a definition of this term.

Administrators

From the PaperVision Enterprise Administration Console, you can set up the following types of administrators

- **Global administrators** can control every aspect of configuration for PaperVision Enterprise, including configurations for all entities. However, they cannot access the documents in a project, as a system (entity) administrator can.
- **System administrators** are entity administrators. They can administrate a single entity and have access to all functionality in all projects for that entity. However, system administrators cannot assign the entity's data group, full-text, migration, and batch paths; these path assignments require a global administrator.
- **Workflow administrators** can design and configure workflows within an entity. They can configure workflow definitions for any project and view workflow history and workflow status reports, but they have no access to documents or functions in any projects unless a system administrator explicitly grants them access. If they have access to view documents within a project, workflow administrators can create workflow instances for a particular document and view its workflow status.
- **Capture administrators** can define capture jobs for use with PaperVision Capture. Capture administrators have no administrative capabilities in PaperVision Enterprise.
- **E-Form administrators** can create E-Forms in PaperVision Enterprise.

Data Group

A data group is a set of documents and their index values. A data group can contain one document or thousands of documents, and those documents can be grouped into one or many projects. A data group holds information for only a single entity, but it can contain an unlimited number of projects. Typically, a data group contains only documents for one project, as this makes organization easier.

Documents

Documents contain the individual pages or images for a given set of index values. If document grouping is enabled, documents are grouped per page results. (See "To set the default document grouping" on page 84 for instructions.) By default, 100 documents appear per page of search results in PaperVision Enterprise.

Detail Sets

Detail sets (also referred to as "duplicate documents") define a collection of index values that allow multiple sets of field data to reference a single document. If documents with detail sets appear in a search results screen in PaperVision Enterprise, they display with a down arrow that allows you to expand all documents contained in the detail set. Detail sets can be created in PaperFlow™, PaperVision Capture, PaperVision Message Manager, and PaperVision Enterprise Report Management.

The example below shows a search results screen with expanded detail sets to show the documents' related Company Name, and Check Date. The Invoice Number and Document ID detail sets vary across documents.

Group by [...]						
	Company Name	Invoice Number	Check Date	@Document ID	@Document Creation Date	@Status
▼	Digitech Systems LLC.	123456	7/26/1997 12:00:00 AM	1	2017-12-18 14:00:16	
	Digitech Systems LLC.	654321	7/26/1997 12:00:00 AM	2	2017-12-18 14:00:16	
▼	Microsoft Inc.	235673	4/4/1975 12:00:00 AM	3	2017-12-18 14:00:16	
	Microsoft Inc.	384745	4/4/1975 12:00:00 AM	4	2017-12-18 14:00:16	
	Microsoft Inc.	893753	4/4/1975 12:00:00 AM	5	2017-12-18 14:00:16	
▼	Amazon Warehouse	737545	7/5/1994 12:00:00 AM	6	2017-12-18 14:00:16	
	Amazon Warehouse	374773	7/5/1994 12:00:00 AM	7	2017-12-18 14:00:16	
	Amazon Warehouse	743723	7/5/1994 12:00:00 AM	8	2017-12-18 14:00:16	
	Amazon Warehouse	823745	7/5/1994 12:00:00 AM	9	2017-12-18 14:00:16	

Entity

An entity is a body such as a company, corporation, or organization. Each entity is autonomous and administers its own projects, users, groups, workflows, security policies, and so on. An entity never shares elements with other entities, and you cannot switch between entities after you log in. A system administrator can limit access to specific projects, functionality, and documents within an entity.

Depending on your configuration, you might be required to log in to your entity from the same computer or network each time.

In general, most users (including those at large enterprise installations) use only a single entity. Only a few special circumstances require more than one entity. For example, in a hosting environment where an application service provider (ASP) is hosting data for multiple companies and each company wants to administrate itself and its users. Digitech Systems' ImageSilo is a good example of an ASP that hosts multiple entities. You might also see more than one entity in a large enterprise consisting of different departments that require the ability to administrate themselves separately from other departments without involving a central IT organization.

Entity ID

An entity ID is a unique number that identifies each entity. Each entity is autonomous. You cannot change your entity ID after you log in and you cannot work across entities.

Index Values

Document index fields contain values that let you identify key elements of documents within a project during the capture process. You then use these index field values to search for and retrieve documents in PaperVision Enterprise. When you enter an index value to perform a search for a document, the application compares the value you entered against your database tables and retrieves documents that meet your specific criteria.



NOTE

When index field values are saved in PaperVision Enterprise, the following characters are automatically removed from them: % ^ & * | <

Project

A project is a logical grouping of documents based on a common indexing schema. For example, ABC Company has three projects: Human Resources, Accounts Receivable, and Sales.

- The Human Resources project contains employee records and health insurance information.
- The Accounts Receivable project contains billing, purchase order, and invoice information.
- The Sales project contains prospect and client information.

Each of these projects is a separate logical grouping within the ABC Company entity. Projects support up to 200 named index fields. Project names must be unique within an entity, but an administrator can create an unlimited number of projects.

Date and Time Format Information

In most cases, dates and times in PaperVision Enterprise display according to the ISO 8601 format. This format describes an internationally accepted way to represent dates and times using numbers. When dates are represented with numbers they can be interpreted in different ways. For example, 01/05/15 could mean January 5, 2015 or May 1, 2015. Following the ISO 8601 format eliminates this uncertainty. The ISO 8601 format orders date and time values so that the largest temporal term (the year) is placed to the left, and then each successively smaller term is placed to the right of the previous term as follows: **YYYY-MM-DD hh:nn:ss**

- **YYYY** indicates a four-digit year, 0000 through 9999
- **MM** indicates a two-digit month of the year, 01 through 12
- **DD** indicates a two-digit day of that month, 01 through 31
- **hh** refers to a zero-padded hour between 00 and 24 (where 24 is only used to denote midnight at the end of a calendar day)
- **nn** refers to a zero-padded minute between 00 and 59
- **ss** refers to a zero-padded second between 00 and 59

Get Product Support

Digitech Systems takes great pride in providing software that is simple to use, feature-rich, and flexible in architecture and integration capabilities. If you experience any difficulty, please contact us toll free at (877) 374-3569 or direct at (402) 484-7777 to experience our legendary customer service. Additionally, you may contact us at support@digitechsystems.com. Our technical support staff is available to serve you between the hours of 8:00 AM and 6:00 PM Central Time.

Digitech Systems' product features and enhancements are driven by you, our customer. If you have an idea for a future product feature or enhancement, please send an e-mail to dev@digitechsystems.com.

In addition to our legendary technical support staff, we also offer the following resources to help you answer questions and resolve issues.

- **MyDSI** - MyDSI is an interactive tool for all Digitech Systems customers. Log in to MyDSI at <http://mydsi.digitechsystems.com> to download product updates, license purchased software, view support contract renewals, and check the status of your software support cases and requests.
- **User Forums** - Log in to the User Forums at <http://forums.digitechsystems.com> to exchange answers and ideas with other users in our moderated community.
- **Knowledge Base** - Log in to search our extensive Knowledge Base at <http://kb.digitechsystems.com> for articles on all Digitech Systems products.
- **Documentation** - For documentation describing the use and features of PaperVision Enterprise, refer to the PaperVision Enterprise product guides. To access the online help and guides from the PaperVision Enterprise software, click the **Help** menu.

Administration Console Access

The Administration Console provides one location where you can perform all administration tasks, including WorkFlow configuration. You can manage an unlimited number of entities from a single sign-on. Only global, system, and WorkFlow administrators can use the Administration Console. See "Administrators" on page 21 for a description of each type of administrator.

To log in to the Administration Console

1. Double-click the **PaperVision Admin Console** icon.
2. In the **Administration Login** dialog box, type your user name and password.
If this is your first time logging in, the user name and password are both **ADMIN**.
3. To log on as a global administrator, select the **Global** check box.
If this is your first time logging in, select the **Global** check box.

To log out of the Administration Console

- On the **Action** menu, select **Exit**.

CHAPTER 2

Global Administration

Global Administration Overview	26
Automation Service Status Tasks	26
Deletion Queue	29
Email Queue	30
Global Administrators	31
Import	33
Licensing	42
Maintenance	44
Migration Jobs	47
Notifications at the Global Level	47
Process Locks	49
Report Management Errors	50
System Settings	50



Global Administration Overview

Only a global administrator can set items located under the **Global Administration** area on the Administration Console. These settings apply to the software as a whole and are separate from entity settings. If a setting exists at the global and entity level, the global setting overrides or sets the limit for the entity setting.

EXAMPLE

For example, there are two settings to specify the maximum amount of idle time for a user session; one is the global system setting **Max. Global Session Idle Time** (located under **System Settings > Configure System Settings > General** tab), and the other is the entity setting **Max. Session Idle Time** (located under **Entity Name > General Security > Security Policy > Configure Security Policy > General** tab). If both of these items are set, the global setting determines the maximum value and the entity setting determines what the value is actually set to, although this value cannot exceed the global setting.

To access global administration settings

- After you have logged in as a global administrator, on the left pane, expand **Global Administration**.

As you work with global administration items, you can use the following three methods to access options.

- Click the **Action** menu, and then select the option.
- On the toolbar, click the icon for the option.
- Right-click the item, and then select the option from the menu that appears.

Automation Service Status Tasks

The PaperVision Enterprise automation service is a Microsoft Windows® service that performs automated tasks at a specified time interval. For each automated task, there is a specific operation to perform it, and you can specify the schedule for each operation. (See "Configure Automation Service Scheduling" on page 61 for information about creating schedules for operations.)

The **Automation Service Status** area displays the current status of all automation servers connected to the PaperVision Enterprise database. You can configure multiple automation service processes to run on a single physical machine. (See "Configure Multiple Automation Service Processes" on page 28 for more information.)

This content describes the automation service tasks you can perform. To perform these tasks you must be logged in to the Administration Console as a global administrator. (See "To log in to the Administration Console" on page 24 if you need help.)

To determine which automated processes are running

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**.

2. Click **Automation Service Status** to display a list of automation server processes and their current state, operation, and date and time.

To start an automation server process

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**.
2. Click **Automation Service Status**.
3. On the right pane, click the server process to start, and then do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Start**.
 - On the toolbar, click **Start**.
 - Right-click the selected item, and then click **Start**.
4. In the **Start Automation Server** dialog box, click **Yes**.

To stop an automation server process

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**.
2. Click **Automation Service Status**.
3. On the right pane, click the server process to stop, and then do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Stop**.
 - On the toolbar, click **Stop**.
 - Right-click the selected item, and then click **Stop**.
4. In the **Stop Automation Server** dialog box, click **Yes**.



N O T E

Performing this task does not stop the current process. However, a command is sent that stops any further processing after the current operation is finished.

To delete an automation server process

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**.
2. Click **Automation Service Status**.
3. On the right pane, click the server process to delete, and then do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Delete**.
 - On the toolbar, click **Delete**.
 - Right-click the selected item, and then click **Delete**.
4. On the **Delete Automation Server** dialog box, click **Yes**.

To refresh an automation server process

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**.
2. Click **Automation Service Status**.

3. On the right pane, click the server process to refresh, and then do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Refresh**.
 - On the toolbar, click **Refresh**.
 - Right-click the selected item, and then click **Refresh**.

Configure Multiple Automation Service Processes

You can configure multiple automation service processes to run on a single physical machine. In this scenario, each automation service process is specified in a `SERVERNAME_INSTANCE` format. The instance sequence starts with zero and increments by one for each added instance.

EXAMPLE

For example, if your system had three simultaneous automation service processes configured on a machine named `SERVER`, the **Automation Service Status** list would show the following under the **Automation Server** column.

```
SERVER_0  
SERVER_1  
SERVER_2
```

Your automation service processes were configured when the software was installed, but you can change the number of simultaneous processes through the configuration utility.

To change the number of simultaneous processes

1. On the applicable machine, start Windows.
2. On the taskbar, click the **Start** button, and then on the **Start** menu, click **All Programs**.
3. Click the **Digitech Systems** folder, and then click **PaperVision Configuration Utility**.
4. If a **User Account Control** dialog box appears, click **Yes** to allow the configuration utility to make changes to the computer.
5. On the left pane of the **PaperVision Configuration Utility**, click **Configure PaperVision Automation Service**.
6. On the right pane, in the **Simultaneous Processes** box, specify the number of the simultaneous processes to use, and then click **Save**.
7. On the **Configure PaperVision Automation Service** dialog box, click **Yes** to restart the service. If you click **No**, you must manually restart the service. Your changes will not take effect until the service has been restarted.

Deletion Queue

Items appear on the **Deletion Queue** when an entity or global administrator submits data groups to be purged by the automation service. (See "Purge Data Groups" on page 117 for more information.) For the automation service to process items on the **Deletion Queue**, you must configure it to do so. See "Configure Automation Service Scheduling" on page 61 for instructions to configure a **Deletion Queue** operation. For each submitted item, the **Deletion Queue** lists the user (and corresponding entity ID) who submitted the purge, the date and time of the submission, and the path that is to be purged.

This content describes the tasks you can perform from the **Deletion Queue** area. To perform these tasks you must be logged in to the Administration Console as a global administrator. (See "To log in to the Administration Console" on page 24 if you need help.)

To view the Deletion Queue

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**.
2. Click **Deletion Queue**.

The right pane shows the user (and corresponding entity ID) who submitted the purge, the date and time of the submission, and the path that is to be purged.

To refresh the Deletion Queue

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**.
2. Click **Deletion Queue**.
3. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Refresh**.
 - On the toolbar, click **Refresh**.
 - Right-click the selected item, and then click **Refresh**.

To delete items from the Deletion Queue

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**.
2. Click **Deletion Queue**.
3. On the right pane, select the item(s) to delete (hold down the Ctrl key to select multiple items), and then do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Delete from Queue**.
 - On the toolbar, click **Delete**.
 - Right-click the selected item(s), and then click **Delete from Queue**.
4. In the **Delete Queue Item** dialog box, click **Yes**.

The item is removed from the **Deletion Queue** and the deletion operation will not be performed.

To manually process an item in the Deletion Queue

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**.
2. Select **Deletion Queue**.

3. On the right pane, select the item to manually process, and then do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Properties**.
 - On the toolbar, click **Properties**.
 - Right-click the selected item, and then click **Properties**.
4. In the **Deletion Queue Item Properties** dialog box, click **Run Now** to remove all of the files in the specified directory.

Email Queue

When email is sent, it is placed in the **Email Queue** to be processed by the automation service for delivery. For the automation service to process items on the **Email Queue**, you must configure it to do so. See "Configure Automation Service Scheduling" on page 61 for instructions to configure an **Email Queue** operation. In addition, there are system settings for configuring email options. See "Email and Notifications System Settings" on page 58 for instructions.

When an item no longer appears in the Email Queue either because it was sent or manually deleted, any associated attachments are removed from the Attachment Path that is specified in system settings. See "Email and Notifications System Settings" on page 58 for more information.

The **Email Queue** lists the email that is waiting to be sent. This content describes the tasks you can perform from the **Email Queue** area. To perform these tasks you must be logged in to the Administration Console as a global administrator. (See "To log in to the Administration Console" on page 24 if you need help.)

To view the Email Queue

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**.
2. Click **Email Queue**.

The right pane shows for each email message: the entity ID from which it was sent, the date and time it was created, the sender and recipient, and the subject.

To view the properties of an item in the Email Queue

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**.
2. Click **Email Queue**.
3. On the right pane, select the item to view, and then do one of the following:
 - Double-click the selected item.
 - On the **Action** menu, point to **All Tasks**, and then click **Properties**.
 - On the toolbar, click **Properties**.
 - Right-click the selected item, and then click **Properties**.

To delete items from the Email Queue

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**.
2. Click **Email Queue**.

3. On the right pane, click the item(s) to delete (hold down the Ctrl key to select multiple items), and then do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Delete**.
 - On the toolbar, click **Delete**.
 - Right-click the selected item(s), and then click **Delete from Queue**.
4. In the **Delete Queue Item** dialog box, click **Yes**.

**N O T E**

When an item no longer appears in the Email Queue either because it was sent or manually deleted, any associated attachments are removed from the Attachment Path that is specified in system settings. See "Email and Notifications System Settings" on page 58 for more information.

To refresh the Email Queue

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**.
2. Click **Email Queue**.
3. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Refresh**.
 - On the toolbar, click **Refresh**.
 - Right-click the selected item, and then click **Refresh**.

Global Administrators

Global administrators can control every aspect of configuration for PaperVision Enterprise, including configurations for all entities. However, they cannot access the documents in a project, as a system (entity) administrator can. You can create and manage global administration accounts from the **Global Administrators** area.

This content describes the tasks you can perform from the **Global Administrators** area. To perform these tasks you must be logged in to the Administration Console as a global administrator. (See "To log in to the Administration Console" on page 24 if you need help.)

To view global administrators

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**.
2. Click **Global Administrators**.

The right pane shows the user and full name for each global administrator.

To create a new global administrator

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**.
2. Click **Global Administrators**.

3. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **New Global Administrator**.
 - On the toolbar, click **New**.
 - Right-click the selected item, and then click **New Global Administrator**.
4. In the **New Global Administrator** dialog box, in the **User Name** box, type the name that will be used to log in.
5. (Optional) In the **Full Name** box, type the user's full name. This name is the one that will be referenced on reports.
6. (Optional) In the **Email Address** box, type an email address for the user.
7. In the **Password** box, type the initial password to access the system. (Passwords are case sensitive.)
8. In the **Confirm Password** box, type the password again to confirm it.



NOTE

We recommend that you never leave a password set to a blank value, as it can pose a security risk.

9. Click **OK**.

To refresh the Global Administrators list

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**.
2. Click **Global Administrators**.
3. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Refresh**.
 - On the toolbar, click **Refresh**.
 - Right-click **Global Administrators**, and then click **Refresh**.

To set a password for a global administrator

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**.
2. Click **Global Administrators**.
3. On the right pane, select the global administrator, and then do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Set Password**.
 - On the toolbar, click **Set Password**.
 - Right-click the selected item, and then click **Set Password**.
4. On the **Set Password** dialog box, in the **New Password** box, type the new password. (Passwords are case sensitive.)
5. In the **Confirm Password** box, enter the password again to confirm it.
6. Click **OK**.

To delete a global administrator

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**.
2. Click **Global Administrators**.
3. On the right pane, select the global administrator, and then do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Delete**.
 - On the toolbar, click **Delete**.
 - Right-click the selected item, and then click **Delete**.
4. On the **Delete Global Administrator** dialog box, click **Yes** to confirm the deletion.

To edit properties of a global administrator

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**.
2. Click **Global Administrators**.
3. On the right pane, select the global administrator, and then do one of the following:
 - Double-click the selected item.
 - On the **Action** menu, point to **All Tasks**, and then click **Properties**.
 - On the toolbar, click **Properties**.
 - Right-click the selected item, and then click **Properties**.
4. On the **Properties** dialog box, you can make changes to the user name, full name, and email address.
5. Click **OK**.



NOTE

The changes take effect the next time the global administrator logs in to the Administration Console.

Import

Data groups are validated during import to verify that all files and required index fields exist. In the entity properties, you can specify whether to halt the import if the data group fails validation. You can also specify to send an email message (instead of the standard notification) with the validation information to entity administrators for import failures and successes. See "Import Entity Properties" on page 79 for instructions to set these options.

Under **Import**, you can access functions to import data groups, monitor their progress, and track import information.

To access import functions

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**.

2. Expand **Import**. For information about the items under **Import**, see the following:
 - See "Import Queue" below for a description of the **Import Queue** and the related tasks you can perform.
 - See "Monitored Import Paths" on page 36 for a description of how monitored import paths work and the related tasks you can perform.
 - See "Import Logs" on page 39 for a description of the **Import Logs** and the related tasks you can perform.

Import Queue

The **Import Queue** lists the data groups that are pending processing by the automation service. Data groups appear on the queue when an administrator manually imports a data group and submits the job to be processed by the automation service, rather than running it immediately. For the automation service to process items on the **Import Queue**, you must configure it to do so. See "Configure Automation Service Scheduling" on page 61 for instructions to configure an **Import Queue** operation.

After the data group is imported, it is automatically removed from the **Import Queue**. If an error occurs during the import process, the error is shown on the **Import Queue**, and the item is disabled. After the problem is resolved, you can enable the item again so that it can be processed. You can also manually disable an import queue item to prevent it from being imported until you enable it. If a data group was erroneously placed on the queue, you can delete it.

This content describes the tasks you can perform from the **Import Queue** area. To perform these tasks you must be logged in to the Administration Console as a global administrator. (See "To log in to the Administration Console" on page 24 if you need help.)

To view the Import Queue

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**.
2. Expand **Import**, and then click **Import Queue**.

The right pane shows for each item: the status, workstation, the date and time of the submission, the path for the data group that is to be imported, the entity name, and the last error that occurred.

To view the properties of an item in the Import Queue

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**.
2. Expand **Import**, and then click **Import Queue**.
3. On the right pane, select the item to view, and then do one of the following:
 - Double-click the selected item.
 - On the **Action** menu, point to **All Tasks**, and then click **Properties**.
 - On the toolbar, click **Properties**.
 - Right-click the selected item, and then click **Properties**.

To refresh the Import Queue

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**.
2. Expand **Import**, and then click **Import Queue**.
3. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Refresh**.
 - On the toolbar, click **Refresh**.
 - Right-click the selected item, and then click **Refresh**.

To delete an item from the Import Queue

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**.
2. Expand **Import**, and then click **Import Queue**.
3. On the right pane, click the item to delete, and then do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Delete**.
 - On the toolbar, click **Delete**.
 - Right-click the selected item, and then click **Delete**.
4. In the **Delete Import Queue Item** dialog box, click **Yes**.

To enable an item on the Import Queue

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**.
2. Expand **Import**, and then click **Import Queue**.
3. On the right pane, click the item to enable, and then do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Enable**.
 - On the toolbar, click **Enable**.
 - Right-click the selected item, and then click **Enable**.
4. In the **Enable Import Queue Item** dialog box, click **Yes**.

To disable an item on the Import Queue

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**.
2. Expand **Import**, and then click **Import Queue**.
3. On the right pane, click the item to disable, and then do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Disable**.
 - On the toolbar, click **Disable**.
 - Right-click the selected item, and then click **Disable**.
4. In the **Disable Import Queue Item** dialog box, click **Yes**.

Monitored Import Paths

To have data imported automatically, you can specify paths for the automation service to monitor. For the automation service to import items that appear in the monitored path, you must configure it to do so. See "Configure Automation Service Scheduling" on page 61 for instructions to configure a **Monitored Import Paths** operation.

While monitoring the specified import paths, the automation service looks for one of the following files:

- DATAGRP.MDB (for PaperFlow data groups)
- COLDGRP.DAT (for DataFlow data groups)
- CDSTAMP.MDB (for Docu-ROM data groups)
- PROJECT.MDB (for ScanTRAX data groups)
- CARFILE.TXT (for C.A.R. data)
- DATAGRP.XML (for XML data groups)
- ERMGROUP.XML (for Report Management data groups)
- MSGGROUP.XML (for Message Capture data groups)
- *.PVPKG (for PaperVision Package Files)

If one of the listed files exists in the root of the monitored import path or in any location below the monitored path, the automation service imports the data group. Therefore, ensure that all of the supporting image and document files for the data group exist before one of the listed files is placed in the monitored path. Take care that the automation service does not begin to import a data group before it is completely transferred.

EXAMPLE

If you are sending an XML data group to a monitored import path via FTP, send all of the supporting image and documents files first. Before you send the DATAGRP.XML file, rename it. For example, change it to DATAGRP.TMP. After the data group is completely transferred, rename the DATAGRP.TMP file back to its original name. Now the automation service will process the new data group.

For the automated imports of XML data groups, Report Management data groups, and PaperVision Enterprise Package Files, a method is provided to prevent the data groups from processing before they are complete. When the automation service locates one of these data groups, it checks for a SUBMIT file in the same directory (DATAGRP.SUBMIT, ERMGROUP.SUBMIT, MSGGROUP.SUBMIT, <PackageFileName>.SUBMIT). If the SUBMIT file does not exist, that data group is left unprocessed until the associated SUBMIT file is copied or created in the same directory as the data group file. The contents of the SUBMIT file are not important; the file can be empty.

This content describes the tasks you can perform from the **Monitored Import Paths** area. To perform these tasks you must be logged in to the Administration Console as a global administrator. (See "To log in to the Administration Console" on page 24 if you need help.)

To view monitored import paths

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**.
2. Expand **Import**, and then click **Monitored Import Paths**.

The right pane shows for each path: the workstation, whether the path is actively being monitored, and the path being monitored for imports.

To create a monitored import path

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**.
2. Expand **Import**, and then click **Monitored Import Paths**.
3. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **New Monitored Import Path**.
 - On the toolbar, click **New**.
 - Right-click the selected item, and then click **New Monitored Import Path**.
4. In the **New Monitored Import Path** dialog box, do one of the following:
 - In the **Path** box, type the path to be monitored.
 - Click the ellipsis button, select the path to be monitored, and then click **Save**.
5. In the **Workstation** area, specify the workstation that will monitor the import path. Select one of the following options:
 - Select **Any** to allow any automation server to monitor the path.
 - Select **Specific** to specify the workstation that will monitor the path, and then do one of the following:
 - Type a specific server name, for example, Server1, or you can type a workstation instance using the *ServerName_Instance* format, for example, typing Server1_14 would allow import paths to be monitored by instance number 14 on Server1.
 - Click the ellipsis button, select the workstation, and then click **OK**.
6. Ensure **Active** is selected for the specified path to be actively monitored. To temporarily disable the monitoring of the path, clear the **Active** check box.
 If the **Active** check box is cleared, the item appears with a red background on the **Monitored Import Paths** window, and the **Active** column displays **Inactive**.
7. Click **OK**.

To refresh monitored import paths

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**.
2. Expand **Import**, and then click **Monitored Import Paths**.
3. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Refresh**.
 - On the toolbar, click **Refresh**.
 - Right-click the selected item, and then click **Refresh**.

To delete a monitored import path

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**.
2. Expand **Import**, and then click **Monitored Import Paths**.
3. On the right pane, select the monitored import path, and then do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Delete**.
 - On the toolbar, click **Delete**.
 - Right-click the selected item, and then click **Delete**.
4. In the **Delete Monitored Import Path** dialog box, click **Yes**.

To modify multiple monitored import paths

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**.
2. Expand **Import**, and then click **Monitored Import Paths**.
3. On the right pane, hold down the Ctrl key, select the monitored import paths to modify, and then do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Modify Paths**.
 - On the toolbar, click **Modify Path**.
 - Right-click the selected items, and then click **Modify Paths**.

A common path is determined for the paths you selected, and this value appears in the **Original Path** box of the **Search and Replace Path** dialog box that appears.

4. In the **Replacement Path** box, do one of the following:
 - Type the replacement path.
 - Click the ellipsis button, select the replacement path, and then click **Save**.
5. Click **Replace**, and then click **Yes** to confirm the change.

To modify the properties of a monitored import path

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**.
2. Expand **Import**, and then click **Monitored Import Paths**.
3. On the right pane, select the monitored import path, and then do one of the following:
 - Double-click the selected item.
 - On the **Action** menu, point to **All Tasks**, and then click **Properties**.
 - On the toolbar, click **Properties**.
 - Right-click the selected item, and then click **Properties**.
4. In the **Monitored Import Path Properties** dialog box, you can make changes to the monitored path, workstation, and specify whether the path is being actively monitored. (See "To create a monitored import path" on the previous page for information about setting each item.)

Import Logs

Import logs record information about the data groups imported manually and by the automation service. In both cases, the global system setting, **Min. Import Log entry age to retain**, controls which log entries are retained based on the number of hours you enter. For example, if this value is set to 48, only the log entries that occurred in the last 48 hours are retained, and all other log entries are archived. See "To set options for log archiving" on page 55 for instructions to specify a value for the **Min. Import Log entry age to retain** setting.

Import log entries can be archived manually and by the automation service. For the automation service to archive import log entries, you must configure it to do so. See "Configure Automation Service Scheduling" on page 61 for instructions to configure a **Report Archiving** operation.

This content describes the tasks you can perform from the **Import Logs** area. To perform these tasks you must be logged in to the Administration Console as a global administrator. (See "To log in to the Administration Console" on page 24 if you need help.)

To view Import Logs

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**.
2. Expand **Import**, and then click **Import Logs**.

The right pane shows for each log entry: the date and time the import was started, whether the import was successful or failed, the entity that received the import, the name of the data group, and the path from which it was imported.

To delete log entries for a date range

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**.
2. Expand **Import**, and then click **Import Logs**.
3. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Delete Range**.
 - On the toolbar, click **Delete Range**.
 - Right-click the selected item, and then click **Delete Range**.
4. In the **Delete Log Entry Range** dialog box, type the date range, and then click **OK**.
5. Click **Yes** to confirm the deletion.

To export log entries for a date range to an XML file

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**.
2. Expand **Import**, and then click **Import Logs**.
3. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Export Range**.
 - On the toolbar, click **Export Range**.
 - Right-click the selected item, and then click **Export Range**.

4. In the **Export Log Entry Range** dialog box, enter the date range, and then click **OK**.
5. In the **Export Log Entries** dialog box, confirm that the date range is correct, and then click **Yes**.
6. In the **Export Log** dialog box, select the location where the export file will go.
7. In the **File Name** box, type a name for the export file, and then click **Save**.

To archive log entries

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**.
2. Expand **Import**, and then click **Import Logs**.
3. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Archive Old Import Logs**.
 - On the toolbar, click **Archive Old Import Logs**.
 - Right-click the selected item, and then click **Archive Old Import Logs**.
4. In the **Archive Import Log Entries** dialog box, confirm that the date and time are correct, and then click **Yes**.

To view import log archives

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**.
2. Expand **Import**, and then click **Import Logs**.
3. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Import Log Archives**.
 - On the toolbar, click **Import Log Archives**.
 - Right-click the selected item, and then click **Import Log Archives**.
4. In the **Import Log Archives** dialog box, click the archive, and then click **View**.

To refresh the Import Logs

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**.
2. Expand **Import**, and then click **Import Logs**.
3. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Refresh**.
 - On the toolbar, click **Refresh**.
 - Right-click the selected item, and then click **Refresh**.

To delete log entries

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**.
2. Expand **Import**, and then click **Import Logs**.
3. On the right pane, select the item to delete (hold down the Ctrl key to select multiple items), and then do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Delete Selected Item(s)**.
 - On the toolbar, click **Delete Selected Item(s)**.
 - Right-click the selected item, and then click **Delete Selected Item(s)**.
4. Click **Yes** to confirm the deletion.

To export log entries to an XML file

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**.
2. Expand **Import**, and then click **Import Logs**.
3. On the right pane, select the item to export (hold down the Ctrl key to select multiple items), and then do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Export Selected Item(s)**.
 - On the toolbar, click **Export Selected Item(s)**.
 - Right-click the selected item, and then click **Export Selected Item(s)**.
4. Click **Yes** to confirm the export.
5. In the **Export Log** dialog box, select the location where the export file will go.
6. In the **File Name** box, type a name for the export file, and then click **Save**.

To view the properties of a log entry

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**.
2. Expand **Import**, and then click **Import Logs**.
3. On the right pane, select the item to view, and then do one of the following:
 - Double-click the selected item.
 - On the **Action** menu, point to **All Tasks**, and then click **Properties**.
 - On the toolbar, click **Properties**.
 - Right-click the selected item, and then click **Properties**.

Licensing

PaperVision Enterprise provides entity, concurrent, and named licenses. Entity licenses are assigned to an entity and are available to any users for that entity. Concurrent licenses are assigned to a specific entity and are restricted to a single user at any given time. Concurrent licenses provide the greatest flexibility since a license is consumed only when a user is logged in to PaperVision Enterprise. If no licenses have been added in the Administration Console, the user receives a messages that no licenses are available. A license is released when a user logs out and when a user session either times out or is “killed” via the **Current Sessions** area in the Administration Console.

Named licenses are assigned per machine or per process and not to individual users. Named licenses are consumed only by the machine or process to which they are assigned. To ensure that a specific machine is always available to process automated tasks, assign a named license to your automation server. In this case, a named license is required for each instance of an automation server.

If you have many licenses to add, you can do a bulk import of them from a text file to save time. To use this feature, contact customer support to get a text file that contains your licensing information, and then go to "To bulk import licenses" on the facing page and complete the procedure.

This content describes the tasks you can perform from the **Licensing** area. To perform these tasks you must be logged in to the Administration Console as a global administrator. (See "To log in to the Administration Console" on page 24 if you need help.)

To view existing licenses

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**.
2. Click **Licensing**.

The right pane shows for each license: the product, version, quantity, serial number, assigned entity, license date, and if applicable, the named system.

To add a new license

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**.
2. Click **Licensing**.
3. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **New License**.
 - On the toolbar, click **New**.
 - Right-click the selected item, and then click **New License**.
4. In the **New License** dialog box, in the **License Code** box, type the license code that was included with your product documentation and media.

5. Do one of the following:
 - Click **Web Authorization** to get the license key online.
 - Click **Phone Authorization**, and then follow the instructions on the **Obtain Authorization Code** dialog box.

**N O T E**

You must provide the serial number and identifier before the license key will be given to you.

6. In the **Obtain Authorization Code** dialog box, type the authorization code, and then click **OK**.

To bulk import licenses

**N O T E**

To use this feature, contact customer support to get a text file that contains your licensing information.

1. If you haven't already done so, contact customer support to get a text file that contains your licensing information.
2. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**.
3. Click **Licensing**.
4. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Import**.
 - On the toolbar, click **Import**.
 - Right-click the selected item, and then click **Import**.
5. In the **Import License File** dialog box, select the text file that contains the license codes to import, and then click **Open**.

Each license code that was successfully imported appears on the right pane. If a license code does not import successfully, a prompt appears asking if you want to do a phone authorization. If you click **Yes**, the **Obtain Authorization Code** dialog box appears with the information you need to complete the authorization by phone.

To refresh the list of licenses

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**.
2. Click **Licensing**.
3. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Refresh**.
 - On the toolbar, click **Refresh**.
 - Right-click the selected item, and then click **Refresh**.

To delete a license

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**.
2. Click **Licensing**.
3. On the right pane, click the license to delete, and then do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Delete**.
 - On the toolbar, click **Delete**.
 - Right-click the selected item, and then click **Delete**.
4. Click **Yes** to confirm the deletion.

To view license properties

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**.
2. Click **Licensing**.
3. On the right pane, select the item to view, and then do one of the following:
 - Double-click the selected item.
 - On the **Action** menu, point to **All Tasks**, and then click **Properties**.
 - On the toolbar, click **Properties**.
 - Right-click the selected item, and then click **Properties**.

Maintenance

Under **Maintenance**, you can access functions to monitor current and completed maintenance tasks.

To access maintenance functions

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**.
2. Expand **Maintenance**. For information about the items under **Maintenance**, see the following:
 - See "Maintenance Queue" below for a description of how the **Maintenance Queue** works and the related tasks you can perform.
 - See "Maintenance Logs" on page 46 for a description of the **Maintenance Logs** and the related tasks you can perform.

Maintenance Queue

The **Maintenance Queue** lists maintenance jobs (such as full-text rebuild, data group encryption, data group moves, etc.) that are pending processing by the automation service. After a maintenance job is processed, it is automatically removed from the queue. For the automation service to process items on the **Maintenance Queue**, you must configure it to do so. See "Configure Automation Service Scheduling" on page 61 for instructions to configure a **Maintenance Queue** operation.

This content describes the tasks you can perform from the **Maintenance Queue**. To perform these tasks you must be logged in to the Administration Console as a global administrator. (See "To log in to the Administration Console" on page 24 if you need help.)

To view the Maintenance Queue

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**.
2. Expand **Maintenance**, and then click **Maintenance Queue**.

The right pane shows for each item: the numeric ID, the date and time of the submission, and a description.

To refresh the Maintenance Queue

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**.
2. Expand **Maintenance**, and then click **Maintenance Queue**.
3. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Refresh**.
 - On the toolbar, click **Refresh**.
 - Right-click the selected item, and then click **Refresh**.

To delete items from the Maintenance Queue

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**.
2. Expand **Maintenance**, and then click **Maintenance Queue**.
3. On the right pane, click the item(s) to delete (hold down the Ctrl key to select multiple items), and then do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Delete**.
 - On the toolbar, click **Delete**.
 - Right-click the selected item(s), and then click **Delete**.
4. Click **Yes** to confirm the deletion.

To view the properties of an item on the Maintenance Queue

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**.
2. Expand **Maintenance**, and then click **Maintenance Queue**.
3. On the right pane, click the item to view, and then do one of the following:
 - Double-click the selected item.
 - On the **Action** menu, point to **All Tasks**, and then click **Properties**.
 - On the toolbar, click **Properties**.
 - Right-click the selected item, and then click **Properties**.

Maintenance Logs

Maintenance logs record information about the maintenance jobs performed by the automation service. See "Configure Automation Service Scheduling" on page 61 for instructions to configure a operations that perform maintenance tasks.

This content describes the tasks you can perform from the **Maintenance Logs**. To perform these tasks you must be logged in to the Administration Console as a global administrator. (See "To log in to the Administration Console" on page 24 if you need help.)

To view the Maintenance Logs

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**.
2. Expand **Maintenance**, and then click **Maintenance Logs**.

The right pane shows for each log entry: the date and time the maintenance job was started, whether the job was successful or failed, a descriptions of the maintenance task, and any associated messages.

To refresh the Maintenance Logs

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**.
2. Expand **Maintenance**, and then click **Maintenance Logs**.
3. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Refresh**.
 - On the toolbar, click **Refresh**.
 - Right-click the selected item, and then click **Refresh**.

To delete log entries

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**.
2. Expand **Maintenance**, and then click **Maintenance Logs**.
3. On the right pane, select the item(s) to delete (hold down the Ctrl key to select multiple items), and then do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Delete**.
 - On the toolbar, click **Delete**.
 - Right-click the selected item, and then click **Delete**.
4. Click **Yes** to confirm the deletion.

To export log entries to an XML file

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**.
2. Expand **Maintenance**, and then click **Maintenance Logs**.

3. On the right pane, select the item(s) to export (hold down the Ctrl key to select multiple items), and then do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Export**.
 - On the toolbar, click **Export**.
 - Right-click the selected item, and then click **Export**.
4. Click **Yes** to confirm the export.
5. In the **Export Maintenance Logs** dialog box, select the location for the placement of the export file.
6. In the **File Name** box, type a name for the export file, and then click **Save**.

To view the properties of a log entry

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**.
2. Expand **Maintenance**, and then click **Maintenance Logs**.
3. On the right pane, click the item to view, and then do one of the following:
 - Double-click the selected item.
 - On the **Action** menu, point to **All Tasks**, and then click **Properties**.
 - On the toolbar, click **Properties**.
 - Right-click the selected item, and then click **Properties**.

Migration Jobs

Migration jobs function the same at the global and entity level. However, as a global administrator, you can see the migration jobs for all entities. See "Migration Jobs" on page 149 at the entity level for more information.

Notifications at the Global Level

Notifications are messages that are usually generated and sent by the system when system events occur that may need your attention. For example, as a global administrator, you receive automated notifications when a data group purge fails. You can also manually send notifications to system users. Whether notifications are created manually or by the system, entity notifications are sent only to entity accounts and global notifications are sent only to global accounts. (See "Notifications at the Entity Level" on page 95 for information about how entity notifications work.) Global notifications can only be accessed via the administration console. Global notifications are sent using the notification method specified under **Global Administration > System Settings > Configure System Settings > Email/Notifications** tab. See "To set the notification method for the global administrator" on page 59 for more information.

To view notifications

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**.
2. Click **Notifications**.

The right pane shows the date and time the notification was sent, and the recipient and source of the notification.

To create a new notification

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**.
2. Click **Notifications**.
3. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **New Notification**.
 - On the toolbar, click **New**.
 - Right-click the selected item, and then click **New Notification**.
4. In the **New Notification** dialog box, from the **Recipient** list, select the person to receive the notification.
5. In the **Message** box, type the message to send, and then click **OK**.

To refresh the list of notifications

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**.
2. Click **Notifications**.
3. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Refresh**.
 - On the toolbar, click **Refresh**.
 - Right-click the selected item, and then click **Refresh**.

To delete an item from the list of notifications

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**.
2. Click **Notifications**.
3. On the right pane, click the item to delete, and then do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Delete**.
 - On the toolbar, click **Delete**.
 - Right-click the selected item, and then click **Delete**.
4. In the **Delete Notification** dialog box, click **Yes**.

To view the properties of a notification

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**.
2. Click **Notifications**.
3. On the right pane, click the notification, and then do one of the following:
 - Double-click the notification.
 - On the **Action** menu, point to **All Tasks**, and then click **Properties**.
 - On the toolbar, click **Properties**.
 - Right-click the selected item, and then click **Properties**.

Process Locks

Process locks prevent multiple components from running the same process. When a component runs a process, it creates a “lock” so that another component cannot start the same process. If a process is unable to complete, for example, if a power failure occurs, the process lock may not be released. In such a case, you may have to manually delete the process lock.

This content describes the tasks you can perform from the **Process Locks** area. To perform these tasks you must be logged in to the Administration Console as a global administrator. (See “To log in to the Administration Console” on page 24 if you need help.)

To view process locks

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**.
2. Click **Process Locks**.

The right pane shows for each process lock: the workstation on which the process is running, the name of the process, and the date and time when the process lock occurred.

To refresh the list of process locks

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**.
2. Click **Process Locks**.
3. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Refresh**.
 - On the toolbar, click **Refresh**.
 - Right-click the selected item, and then click **Refresh**.

To delete a process lock

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**.
2. Click **Process Locks**.
3. On the right pane, click the process lock to delete, and then do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Delete**.
 - On the toolbar, click **Delete**.
 - Right-click the selected item, and then click **Delete**.
4. Click **Yes** to confirm the deletion.

Report Management Errors

Report Management Errors function the same at the global and entity level. However, as a global administrator, you can see the Report Management Errors for all Report Management Jobs for all entities. See "Report Management Errors" on page 254 for more information.

System Settings

Under **System Settings**, you can configure global system settings and the schedule for the automation service.

To access system settings functions

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**.
2. Click **System Settings**. For information about the items that appear on the right pane, see the following:
 - See "Configure System Settings" below for an overview of system settings and how to set them.
 - See "Configure Automation Service Scheduling" on page 61 for a description of automation services and how to configure them.

Configure System Settings

System settings configure operations that are global and not specific to a particular entity. Settings not marked as local are globally distributed through the centralized database. Local settings are specific to the computer on which they are set, so if you are using multiple web or application servers, you must specify the local settings for each one. The system settings content describes the tasks you can perform from the **Configure System Settings** area. To perform these tasks you must be logged in to the Administration Console as a global administrator. (See "To log in to the Administration Console" on page 24 if you need help.)

To access system settings

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**, and then click **System Settings**.
2. On the right pane, double-click **Configure System Settings**.

The **System Settings** dialog box appears with tabs that organize the system settings into categories. For information about the settings on each tab, see the following:

- See "General System Settings" on the facing page for information to specify settings on the **General** tab.
- See "Data System Settings" on page 53 for information to specify settings on the **Data** tab.
- See "Replication System Settings" on page 56 for information to specify settings on the **Replication** tab.
- See "Email and Notifications System Settings" on page 58 for information to specify settings on the **Email/Notifications** tab.
- See "Local System Settings" on page 60 for information to specify settings on the **Local** tab.

General System Settings

General system settings let you configure options for utilization limits, server-side processing, reports/notifications, encryption, and communication. Each option is described in the following procedures.

To set utilization limits

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**, and then click **System Settings**.
2. On the right pane, double-click **Configure System Settings**.
3. Click the **General** tab.
4. In the **Utilization Limits** area, you can set the following items:
 - **Max. SQL database results per query** - This setting specifies the maximum number of documents returned for a search. If document grouping is enabled, fewer documents may be returned because some documents may be grouped to appear as one.
 - **Max. Full-Text database results per query** - This setting specifies the maximum number of full-text search items returned by the full-text search engine.
 - **Max. Global Session idle time (minutes)** - This global setting specifies the maximum number of minutes that a user session can remain idle before the automation service automatically logs the user out of the system. You can also set this value at the entity level (with the **Max. Session Idle Time** setting under **Entity Security Policy**). If both of these items are set, the global setting determines the maximum value, and the entity setting determines what the value is actually set to, although this value cannot exceed the global setting.
 - **Max. Workflow History Size (characters)** - This setting specifies the maximum size (in characters) that a WorkFlow instance history can reach before an alert is generated. This setting can help you identify workflows that erroneously loop through the same set of worksteps before they cause performance issues on the database server.

To set options for server-side processing

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**, and then click **System Settings**.
2. On the right pane, double-click **Configure System Settings**.
3. Click the **General** tab.
4. In the **Server-Side Processing** area, you can set the following items:
 - **Disregard WorkFlow Task Server Operations** - If selected, automated WorkFlow tasks (such as **Launch Application/Shell** and **Raise Event**) are prevented from running on automation servers. These tasks could pose security problems, for example, a launch operation that deletes files.

- **Disregard E-Forms Server-Side Custom Code** - If selected, E-Forms custom code is prevented from running on automation servers. Each E-Form that uses custom code must have an engine specified to run the custom code. To specify the custom code engine on the **E-Form Designer**, on the top of the **Properties** pane, click the down arrow, select **Form**. In the **General** group, select **Custom Code Engine**, and then click the ellipsis button to open the **Custom Code Engine Mode** dialog box, select one of the following options to run the custom code for the form:
 - Select **PaperVision E-Forms Custom Code Server** to run the code from the PaperVision Enterprise server site.
 - Select **PaperVision Assistant** to use the PaperVision assistant to communicate with the PaperVision Enterprise server and process the code on the client system where the PaperVision Assistant is installed.



NOTE

Selecting **Disregard E-Forms Server-Side Custom Code** will not prevent E-Forms custom code from running when the **PaperVision Web Assistant** option is selected. Because the custom code is processed on the client and does not pose a security risk to the server, it is allowed to run.

- Select **External Server URL**, and then specify the location. The **PaperVision Enterprise External Custom Code Server** is available on the **Downloads** tab.

To set the maximum number of display items for reports/notifications

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**, and then click **System Settings**.
2. On the right pane, double-click **Configure System Settings**.
3. Click the **General** tab.
4. In the **Reports/Notifications** area, you can set the following item:
 - **Max. Report/Notification items to display** - This setting specifies the maximum number of records returned in a report or notification list. Use this setting to ensure that large reports and notification lists do not overburden the database server.

To set the server-side encryption key

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**, and then click **System Settings**.
2. On the right pane, double-click **Configure System Settings**.
3. Click the **General** tab.
4. In the **Encryption** area, you can set the following item:
 - **Server-Side Encryption Key** - This setting specifies the encryption key used to encrypt all server-side communications. If you do not specify an encryption key, a default key is used. As such, we strongly recommend that you specify this value.

To set the client ping increment

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**, and then click **System Settings**.
2. On the right pane, double-click **Configure System Settings**.

3. Click the **General** tab.
4. In the **Communication** area, you can set the following item:
 - **Client Ping Increment (secs)** - This setting specifies the interval in seconds between each "ping" the client application sends to the server. When a user logs in, if their client application can ping the server, the server instructs it to do so at the interval specified here. This background ping verifies that the client application is open and keeps the user session active. If a client has not sent the expected ping within 60 seconds of the specified ping interval, the session is automatically terminated. This feature releases licenses used by applications that were closed without logging out the user. Without ping validation, the user session does not terminate until the session times out.

**N O T E**

Because some mobile browsers do not support background operations, the **Client Ping Increment** setting does not apply to Android and iPad devices. For these devices, the **Max Session Idle Time** setting for the entity determines the session length.

Data System Settings

Data system settings let you configure options for data processing, data size management, Report Management, and log archiving. Each option is described in the following procedures. (Options that affect data can also be set at the entity level. See "Import Entity Properties" on page 79 for more information.)

To set data processing items

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**, and then click **System Settings**.
2. On the right pane, double-click **Configure System Settings**.
3. Click the **Data** tab.
4. In the **Data Processing** area, you can set the following items:
 - **Disable data group sizing** - If selected, the system does not log the amount of storage used as data groups are imported. This logging can be time consuming for large data groups, but it provides valuable information for managing storage resources.
 - **Force copy and delete of imported data groups** - If selected, this setting overrides the entity-level settings for importing data groups and forces data groups to be copied during import. (See "To set data group auto-mapping" on page 83 for information about entity-level settings for imports.) The global administrator can ensure that all documents are stored in their appropriate location. Selecting this setting can be particularly useful in situations where the data groups are being imported from an FTP site.

- **Full/reload imports compare last modified dates** - If selected, during a full/reload import, the system compares the last modified date of the DATAGRP.MDB file (that contains the main database/XML for the data group) to the last modified date of the previous import. If the file was not modified, then the import is skipped. If this setting is not selected, the modification dates are compared only when an append import operation is performed.



NOTE

At the entity level, if you perform an immediate and manual full/reload import of a data group, the system ignores this setting and imports the data group regardless of the file modification date.

- **Force purged data group deletion** - If selected, when a data group is purged, the files are always removed from the storage media, regardless of the state of the data group. If this setting is not selected, when a data group is purged, only data groups that have a **Read/Write** state are removed, and those with a **Read-Only** state are retained.
- **Purge data groups during entity deletion** - If selected, data groups that have a **Read/Write** state are automatically submitted to be purged, and are deleted from the storage media when the entity is deleted.
- **Require 'dirmgr.submit' files for directory manager job processing** - If selected, the directory manager operation runs only when a `dirmgr.submit` or `packagefilename.submit` file exists at the root path for the import job. The content of the submit file is irrelevant, as it is not imported as part of the job. Checking for this file ensures that the directory manager does not run while files are being transmitted which can cause issues.
- **Clear package workspace prior to each use** - If selected, the system clears the package workspace prior to importing a data group from a package file, or running a backup or directory manager job. If a failure occurs during one of these operations, setting this option clears the workspace of failed data.
- **Enable data group mapping** - If selected, auto-mapping occurs for data groups that are imported automatically. Selecting this option causes the automation service to look for a mapping file (`datagrps-map.xml`) when importing a data group. If the mapping file exists, the data group is automatically mapped by creating an association between the CLIENTID and the entity. If the mapping file exists, but auto mapping cannot be performed, an error is generated and the data group is not imported. This option is selected by default. (See "Import Entity Properties" on page 79 for information about setting data group auto-mapping properties at the entity level.) Clearing this option globally disables auto-mapping if you need to load data groups that have an auto-map file for a different entity ID.
- **Delete source data group files after move** - If selected, source data group files are deleted after they are successfully moved.

To set options for data size management

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**, and then click **System Settings**.
2. On the right pane, double-click **Configure System Settings**.
3. Click the **Data** tab.

4. In the **Data Size Management** area, you can set the following items:
 - **Max. Attachment Data Group Size (MB)** - This setting specifies the maximum size (in megabytes) that an attachment data group can reach before a new one is automatically created. If this option is set to zero, no size limit is enforced.
 - **Max. Backup Package Contents Size (MB)** - This setting specifies the maximum size (in megabytes) of content placed in a backup package during a project-level backup. When the maximum size is reached, the system creates a new package file.

**N O T E**

This setting does not specify the size of the package file, but the size of its contents before compression.

To set options for Report Management

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**, and then click **System Settings**.
2. On the right pane, double-click **Configure System Settings**.
3. Click the **Data** tab.
4. In the **Report Management Settings** area, you can set the following items:
 - **Max. Documents per File Set** - This setting specifies the maximum number of documents the Report Management Operation processes for a file set before it is imported. During the extraction of detail field data, this value might be exceeded to ensure that this information writes to the same file set.
 - **Delete Source on Success** - If selected, the source file is deleted after it is successfully parsed through the Report Management Operation. Otherwise, the file is moved to the **Successfully Processed** folder in the directory specified in the **Report Management Path** setting. (See "Local System Settings" on page 60 for instructions to set the Report Management Path.)
 - **Require Submit File** - If selected, the Report Management Operation processes only files that have a corresponding file with a `.submit` extension. For example, to process a file named `test.txt` a `test.txt.submit` file must exist. The content of the submit file is irrelevant, as it is not imported as part of the job. The main file is sent to the job's input path, but will not be parsed until the submit file is also delivered. Checking for the submit file prevents the main file from being processed before it is completely transferred.

To set options for log archiving

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**, and then click **System Settings**.
2. On the right pane, double-click **Configure System Settings**.
3. Click the **Data** tab.

4. In the **Log Archiving** area, you can set the following items:
- **Min. Import Log entry age to retain (hours)** - This setting specifies which log entries are retained based on the number of hours you enter. For example, if this value is set to 48, only the log entries that occurred in the last 48 hours are retained, and all other log entries are archived. As import logs are archived, database records are removed and placed in a textual XML document. You cannot search these textual XML documents from PaperVision Enterprise, but you can access the data using a separate application. Consider leaving the most recent records in the database for easy review access.
 - **Number of Security Log entries to retain** - This setting specifies the number of security log entries to retain in the database. As security logs are archived, database records are removed and placed in a textual XML document. You cannot search these textual XML documents from PaperVision Enterprise, but you can access the data using a separate application. Consider leaving the most recent records in the database for easy review access.

Replication System Settings

You can replicate your data on another server and/or site for backup and high-availability applications. You can replicate data to as many locations as necessary, either locally or across WAN connections to separate sites. The replication process uses a journal method. When a system attaches a new document, checks in a new document version, deletes a document, imports data groups, purges data groups, or deletes projects, the system checks for a defined journal entry path. If one exists, a journal entry (a specially formatted text file) is written to the location. The journal entry records the type of operation performed and on which files or directories.

The actual replication process occurs on a machine (or multiple machines) running as a PaperVision automation server that has the **File Replication** operation configured. (See "Configure Automation Service Scheduling" on page 61 for instructions to configure a **File Replication** operation.) This operation accesses the defined journal entry paths, creates a list of the journal entries, and then sorts them by the date and time they were created. Each entry is then processed, replicating the same operation to all of the defined replication journal entry paths. If an error occurs during a replication process, an entry that specifies the operation and line where the error occurred is written to the journal file. The journal file is renamed to prevent it from processing again, and a copy of the file is placed on the local machine in the **Digitech Systems\Common Files\JournalErrors** directory where PaperVision Enterprise is installed. After the error is resolved, rename the file by removing the .ERROR extension to have the file processed.

Replication system settings let you define replication destination paths and replication journal entry paths. Setting up these replication paths is described in the following procedures.

Replication Destination Paths

When the replication process occurs on the PaperVision Enterprise automation server, files are replicated to the destination paths that you specify.



I M P O R T A N T

We recommend that you use Universal Naming Convention (UNC) paths (for example, `\\Servername\Sharename`) and ensure that the service account used on the automation server has full read/write access to the shares.

To add replication destination paths

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**, and then click **System Settings**.
2. On the right pane, double-click **Configure System Settings**.
3. Click the **Replication** tab.
4. In the **Replication Destination Path(s)** area, click **Add**.
5. In the **Add Replication Destination Path** dialog box, do one of the following:
 - In the **Path** box, type the location where the replication files will go.
 - Click the ellipsis button, select the replication destination path, and then click **OK**.
 - Click the ellipsis button, and then click **Current User** to create a folder under the selected directory. If you want to, rename the folder, and then click **OK**.
6. Click **OK** to add the path.

To delete replication destination paths

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**, and then click **System Settings**.
2. On the right pane, double-click **Configure System Settings**.
3. Click the **Replication** tab.
4. In the **Replication Destination Path(s)** area, select the path(s) to delete.
5. Click **Delete**, and then click **Yes** to confirm the deletion.

Replication Journal Entry Paths

For each server that will perform any operation that requires a replication journal entry, you must specify a replication journal entry path. This location does not need to be unique to each server. However, using separate, local, shares on each server preserves replication data if the server holding the replication journals becomes unavailable.



I M P O R T A N T

We recommend that you use Universal Naming Convention (UNC) paths (for example, `\\Servername\Sharename`) and ensure that the service account used on the automation server to perform replications has full read/write access to the shares.

To add replication journal entry paths

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**, and then click **System Settings**.
2. On the right pane, double-click **Configure System Settings**.
3. Click the **Replication** tab.
4. In the **Replication Journal Entry Path(s)** area, click **Add**.
5. In the **Replication Journal Path Properties** dialog box, do one of the following:
 - In the **Server** box, type the name of the application server that will write the journal entries.
 - Click the ellipsis button next to the **Server** box, select the application server that will write the journal entries, and then click **OK**.

6. In the **Replication Journal Path Properties** dialog box, do one of the following:
 - In the **Path** box, type the journal output path for the server.
 - Click the ellipsis button next to the **Path** box, select the journal output path for the server, and then click **OK**.
 - Click the ellipsis button, and then click **Current User** to create a folder under the selected directory. If you want to, rename the folder, and then click **OK**.
7. Click **OK** to add the properties for the replication journal entry path.

To edit a replication journal entry path

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**, and then click **System Settings**.
2. On the right pane, double-click **Configure System Settings**.
3. Click the **Replication** tab.
4. In the **Replication Journal Entry Path(s)** area, select the path, and then click **Edit**.
5. In the **Replication Journal Path Properties** dialog box, you can make changes to the server and path. (See "To add replication journal entry paths" on the previous page for information about setting each item.)

To delete replication journal entry paths

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**, and then click **System Settings**.
2. On the right pane, double-click **Configure System Settings**.
3. Click the **Replication** tab.
4. In the **Replication Journal Entry Path(s)** area, select the path(s) to delete.
5. Click **Delete**, and then click **Yes** to confirm the deletion.

Email and Notifications System Settings

Email and notification system settings let you configure options for email and the method used to send notifications to the global administrator. Each option is described in the following procedures.

To configure email settings

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**, and then click **System Settings**.
2. On the right pane, double-click **Configure System Settings**.
3. Click the **Email/Notifications** tab.
4. In the **Email Settings** area, you can set the following items:
 - **SMTP Server Name/IP** - This setting specifies the SMTP server name or IP address the system will use to send emails.
 - **SMTP Server Port** - This setting specifies the port number used to communicate with the SMTP server. The default value is 25.
 - **SMTP User Name** - This setting specifies a valid user name if the SMTP server requires authentication prior to sending an email.

- **SMTP Password** - This setting specifies the password if the SMTP server requires authentication prior to sending an email.
- **SMTP Encryption** - This setting specifies the type of SMTP encryption the system will use to send emails.
 - **None** - This setting uses no SSL security. All communication occurs in plain text mode. This is the default setting.
 - **SSL Automatic** - This setting specifies that if the remote port is set to the standard plain text port of the protocol, the system will use SSL Explicit encryption. In all other cases, the system will use SSL Implicit encryption.
 - **SSL Explicit** - The setting specifies that the system will first connect in plain text, and then explicitly start SSL negotiation through a protocol command such as STARTTLS.
 - **SSL Implicit** - This setting specifies that the system will immediately start SSL negotiation after a connection is established.
- **Send Email From** - This setting specifies the email address from which automated emails are sent.
- **Attachment Path** - This setting specifies the path used by the automated email process to temporarily store email attachments until the email is sent. Ensure that this path is accessible from all PaperVision Enterprise servers that send and generate emails (for example, through automated WorkFlow tasks). We recommend that you use a Universal Naming Convention (UNC) path (for example, \\Servername\Sharename). To set the attachment path, do one of the following:
 - In the **Attachment Path** box, type the attachment path.
 - Click the ellipsis button, select the attachment path, and then click **OK**.
 - Click the ellipsis button, and then click **Current User** to create a folder under the selected directory. If you want to, rename the folder, and then click **OK**.

**N O T E**

If an email message is deleted from the **Email Queue**, either because it was sent or manually deleted, any associated attachments are removed from the attachment path.

5. (Optional) To test your settings, click **Send Test Message**.

To set the notification method for the global administrator

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**, and then click **System Settings**.
2. On the right pane, double-click **Configure System Settings**.
3. Click the **Email/Notifications** tab.
4. In the **Global Administrator Notification Method** area, select one of the following items:
 - **Publish Notification** - If selected, notifications are published in the database and accessed from the Administration Console by expanding **Global Administration**, and then clicking **Notifications**.

- **Send Email** - If selected, notifications are sent via email to the global administrator's email address that is specified for the user account.
- **Publish Notification and Send Email** - If selected, notifications are published and sent via email as described in the previous two options.

Local System Settings

Local settings are specific to the machine on which they are configured. If your site has multiple application or automation servers installed, you must configure the local settings for each server. Each option for local system settings is described in the following procedures.

To configure local settings

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**, and then click **System Settings**.
2. On the right pane, double-click **Configure System Settings**.
3. Click the **Local** tab.
4. In the **Local Settings** area, you can set the following items:
 - **Web File Cache Path** - This setting specifies the full path to the location where files are cached when they are retrieved. If your site uses multiple web servers, unique cache settings for each one are not required. You can use identical cache settings that all point to the same network share. We recommend that you use a Universal Naming Convention (UNC) path (for example, `\\Servername\Sharename`). For high availability, you can specify multiple paths separated by a pipe character (`|`). If the server cannot access the first location, it moves the inaccessible path to the end of the list, and then tries the next path. This process repeats until the server can cache the file to one of the specified paths. To set the web file cache path, do one of the following:
 - In the **Web File Cache Path** box, type the path.
 - Click the ellipsis button, select the path, and then click **OK**.
 - Click the ellipsis button, and then click **Current User** to create a folder under the selected directory. If you want to, rename the folder, and then click **OK**.
 - **Web File Cache URL** - This setting specifies the URL where the path in the **Web File Cache Path** box is located. If you specified multiple paths, you must specify the same number of URLs separated by a pipe character (`|`).
 - **Primary Web Server URL** - This setting only requires a value if the web servers are behind a load balancer. If the web server URL uses ports, do not include them in this URL.
 - **Package Workspace** - This setting specifies the temporary location for package files that are created for backup or import jobs. Ensure that this location has ample space to temporarily hold the extracted contents of imported package files and any package file being processed.
 - **Report Management Path** - This setting specifies the path where the Report Management Operation writes created files sets and their temporary cache files. After the file set is completed, it is copied into a data group and removed from this location. Processed files are copied to the **Successfully Processed** or **Failed to Process** directories under this path.

To configure automation service logging

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**, and then click **System Settings**.
2. On the right pane, double-click **Configure System Settings**.
3. Click the **Local** tab.
4. In the **Automation Service Logging** area, you can set the following items:
 - **Enable Logging** - If selected, logging for the automation service is turned on. This information is helpful for troubleshooting processes performed by the automation service.
 - **Log Path** - This setting specifies the path where the log files for the automation service are written.

Configure Automation Service Scheduling

The automation service automatically runs the operations you add to its schedule. For each operation, you can configure the start time, schedule, and the rate of repetition. Where operations appear on the **Automation Service Schedule** determines the order in which the automation service evaluates them. When the automation service evaluates the operations, it begins with the item at the top of the schedule and compares the value listed in the **Next Run Time** column to the current date and time. If the **Next Run Time** is earlier than the current date and time, it moves to the next operation in the schedule. If the **Next Run Time** value is equal to or later than the current date and time, the automation service runs the operation, records the run time in the **Last Run Time** column, and then sets the value in the **Next Run Time** column based on the schedule you specified for the operation. The automation service then repeats this process with the next operation on the schedule. When you modify the **Automation Service Schedule**, your changes take effect as soon as you save them.

This content describes the tasks you can perform from the **Configuring Automation Service Scheduling** area. To perform these tasks, you must be logged in to the Administration Console as a global administrator. (See "To log in to the Administration Console" on page 24 if you need help.)

Available Operations

The following operations are available for you to configure:

- **Backup Processing** - This operation performs scheduled backup jobs.
- **Deletion Queue** - This operation deletes items in the **Deletion Queue** that were submitted by data group purges.
- **Directory Manager Jobs** - This operation processes any jobs that appear as **Active** in the **Directory Manager Jobs** list. (See "Directory Manager Jobs" on page 193 for more information.)
- **Email Queue** - This operation processes items in the **Email Queue**.
- **File Replication** - This operation replicates any journal entries in the **Replication Journal Entry Paths** to the specified **Replication Destination Paths**. (See "Replication System Settings" on page 56 for more information.)

- **Full-Text Index Compression** - This operation compresses the full-text database indexes to regain lost space. Lost space is created when documents or data groups that have data in the full-text database are deleted. Although the data is removed from the full-text database, the disk space used by that data is not recovered. Running this operation recovers the lost space.



N O T E

Do not schedule the **Full-Text Index Compression** operation to run on a frequent, regular interval, as it places a significant processing load on the server.

- **Full-Text Replication** - This operation replicates all full-text databases to all specified **Replication Destination Paths**. (See "Replication System Settings" on page 56 for more information.)
- **Import Queue** - This operation imports data groups listed on the **Import Queue**. (See "Import Queue" on page 34 for more information.)
- **Maintenance Queue** - This operation processes any maintenance jobs listed on the **Maintenance Queue**. (See "Maintenance Queue" on page 44 for more information.)
- **Migration Jobs** - This operation processes any migration jobs listed on the **Migration Jobs** pane. (See "Status and Tasks for Submitted Migration Jobs" on page 150 for more information.)
- **Monitored Import Paths** - This operation checks the directories specified in the **Monitored Import Paths** list and immediately imports any data groups found in them. (See "Monitored Import Paths" on page 36 for more information.)
- **Monitored Import Paths (Submit)** - This operation checks the directories specified in the **Monitored Import Paths** list and places any data groups found in them on the **Import Queue** rather than importing them immediately. (See "Monitored Import Paths" on page 36 and "Import Queue" on page 34 for more information.) This operation minimizes the network and storage system impact caused by having a large number of automation servers searching paths for data groups to import.
- **Records Retention** - This operation processes the active records retention policy sets for each project under each entity. For retention policies, only documents that are not locked are evaluated. For destruction policies, only documents that are not marked for destruction or review are evaluated. After the documents are evaluated, the operation applies the retention (lock) or destruction (deletion) date and time to documents according to the criteria specified in the records retention policy set. (See "Records Retention Policy Sets" on page 200 for more information.) Documents that have destruction (deletion) dates and times that are earlier than the current date and time are deleted.
- **Recycle Bin** - This operation deletes items in the Recycle Bin when the **Automatically Empty Recycle Bin** setting is configured in the project properties. (See the "To edit project properties" on page 162 procedure for information about Recycle Bin settings.) Documents emptied from the Recycle Bin are removed from the full-text database, folders, and workflow instances. In addition, object files, annotations, and signatures are removed. When items are deleted from the Recycle Bin, the **Emptied Recycled Document** operations are logged in the document access report.

- **Report Archiving** - This operation archives the **Document Access** and **System Operations/Queries** reports, and entries from the **Import Logs**. To retain items in the **Document Access** and **System Operations/Queries** reports, specify a value for the **Number of Security Log entries to retain** setting. Otherwise, all entries for these reports are archived. To determine which entries are retained in the **Import Logs**, specify a value for the global system setting, **Min. Import Log entry age to retain**. It controls which log entries are retained based on the number of hours you enter. For example, if this value is set to 48, only the log entries that occurred in the last 48 hours are retained, and all other log entries are archived. (See "To set options for log archiving" on page 55 for instructions to specify the **Number of Security Log entries to retain** and the **Min. Import Log entry age to retain** settings.)
- **Report Management** - This operation processes the configured, active jobs listed in the **Report Management Jobs** area. (See "Report Management Overview" on page 224 for more information.)
- **Session/Grant Cleanup** - This operation removes sessions that have remained idle longer than the value specified by the **Max. Session Idle Time** setting for the entity. (See "To set the maximum session idle time" on page 138 to specify this setting.) This operation also removes expired document grants.
- **Storage Utilization Snapshots** - This operation reads and records the storage in use by each entity. Each time it runs, it creates a "snapshot" that represents a sample in the utilization report for the entity. (See "Utilization" on page 302 for information about this report.)
- **Workflow (Automated)** - This operation takes ownership of worksteps, and then completes worksteps in any workflows that have a participant marked as <Automated>. (See "Automated Worksteps" on page 261 for more information.)
- **Workflow (Max. Times)** - This operation processes all active worksteps with expired time limits, sends the appropriate notifications, and transitions to new worksteps as defined. (See "Automated Worksteps" on page 261 for more information.)
- **Workflow (Pre-Conditions)** - When this operation runs, it looks for any pre-conditions defined with the **Document Selection Method** set to **Criteria for Automated WorkFlow (Pre-Condition)**. If any documents meet the criteria, the WorkFlow instance is created and the document is marked so that WorkFlow definitions will no longer be processed against the document. (See "To add a pre-condition to a workflow definition" on page 269 for more information.)

To open the Automation Service Schedule

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**.
2. Click **System Settings**.
3. On the right pane, double-click **Configure Automation Service Scheduling**.

The **Automation Service Schedule** area displays the name of the operation, the schedule on which it runs, the next run time, the last run time, and the resulting status of the operation after the last run time.

To add an automation service operation

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**.
2. Click **System Settings**.

3. On the right pane, double-click **Configure Automation Service Scheduling** to open the **Automation Service Scheduling** dialog box.
4. If your site is configured to use multiple automation servers, from the **Automation Server** list, select the server that will run the configured operations.
5. Click **Add** to open the **New Automation Service Schedule** dialog box.
6. From the **Operation** list, select the operation to add to the **Automation Service Schedule**.
(See "Available Operations" on page 61 for a description of each operation in the list.)
7. In the **Start Time** box, type the date and time for the operation to start running according to the schedule you are setting up.

By default, this box displays the date and time when you clicked **Add**. (See "Date and Time Format Information" on page 23 if you need help understanding the correct date and time format to use.)
8. From the **Schedule** list, select the unit of time on which to base the schedule.

The option in the **Repetition Schedule** area is automatically updated to reflect your selection.
9. In the **Repetition Schedule** area, specify the frequency of repetition for the operation.
10. Click **OK** to add the operation to the **Automation Service Schedule**.
11. Click **Save** to save your changes, and then click **OK** on the confirmation message.

To edit an automation service operation

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**.
2. Click **System Settings**.
3. On the right pane, double-click **Configure Automation Service Scheduling** to open the **Automation Service Scheduling** dialog box.
4. In the **Automation Service Schedule** area, click the operation to modify, and then click **Edit**.
5. In the **Edit Automation Service Scheduling** dialog box, you can change the operation, its start time, schedule, and rate of repetition. (See "To add an automation service operation" on the previous page for information about setting each item.)
6. Click **Save** to save your changes, and then click **OK** on the confirmation message.

To change the evaluation order for an automation service operation

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**.
2. Click **System Settings**.
3. On the right pane, double-click **Configure Automation Service Scheduling** to open the **Automation Service Scheduling** dialog box.
4. In the **Automation Service Schedule** area, click the operation to move, and then use the arrow buttons to move the operation up or down.

When the automation service evaluates the operations, it begins with the item at the top of the schedule and then moves down through the listed operations.
5. Click **Save** to save your changes, and then click **OK** on the confirmation message.

To remove an automation service operation

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**.
2. Click **System Settings**.
3. On the right pane, double-click **Configure Automation Service Scheduling** to open the **Automation Service Scheduling** dialog box.
4. In the **Automation Service Schedule** area, click the operation to remove, and then click **Remove**.
5. Click **Yes** to confirm the removal of the operation from the schedule.
6. Click **Save** to save your changes, and then click **OK** on the confirmation message.

View Full-Text Queue Statistics

Global administrators can run a report that shows the items in the full-text queue at the time the report is run. The results are presented in XML, and show the items in the queue separated by Entity ID, Project ID, and Process Type.

To view full-text queue statistics

1. After you have logged in to the Administration Console as a global administrator, on the left pane, expand **Global Administration**.
2. Click **System Settings**.
3. On the right pane, double-click **View Full-Text Queue Statistics** to view the statistics in a browser window.

This page was intentionally inserted without content.



CHAPTER 3

Entity Configuration

Entity Configuration Tasks	68
----------------------------------	----



Entity Configuration Tasks

An entity is a body such as a company, corporation, or organization. Each entity is autonomous and administers its own projects, users, groups, workflows, security policies, and so on. An entity never shares elements with other entities, and you cannot switch between entities after you log in. A system administrator can limit access to specific projects, functionality, and documents within an entity. Depending on your configuration, you might be required to log in to your entity from the same computer or network each time.

In general, most users (including those at large enterprise installations) use only a single entity. Only a few special circumstances require more than one entity. For example, in a hosting environment where an application service provider (ASP) is hosting data for multiple companies and each company wants to administrate itself and its users. Digitech Systems' ImageSilo service is a good example of an ASP that hosts multiple entities. You might also see more than one entity in a large enterprise consisting of different departments that require the ability to administrate themselves separately from other departments without involving a central IT organization.

When you add an entity, the system automatically assigns it an entity ID number. The numbering system starts at one and automatically increments each time you add an entity. If you delete an entity, its ID number is never reused. You can use the entity ID number to search for an entity. (See "To add a new entity" below and "To find an entity ID" on the facing page for more information.)

If your site uses multiple entities, you can change the data group path for all of them at the same time. (See "To change data group paths for all entities" on the facing page for more information.) This feature is helpful when new storage is needed, as you don't have to individually change the path for each entity. Keep in mind that this feature applies only to data groups that are imported or created after you modify the path, and has no effect on existing data groups.

This content describes the tasks you can perform from the **Entities** area. To perform these tasks you must be logged in to the Administration Console as a global administrator. (See "To log in to the Administration Console" on page 24 if you need help.)

To view existing entities

- After you have logged in to the Administration Console as a global administrator, on the left pane, click **Entities**.

The right pane shows for each entity: the entity ID, name, and the date it was created.

To add a new entity

1. After you have logged in to the Administration Console as a global administrator, on the left pane, click **Entities**.
2. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **New Entity**.
 - On the toolbar, click **New**.
 - Right-click the selected item, and then click **New Entity**.
3. On the **General** tab, in the **Entity Name** box, type a name for the entity.

- Specify the properties on each tab in the **New Entity** dialog box.

**N O T E**

At a minimum, you must specify the **Database Settings** and the **Entity Paths** on the **General** tab before the system will add the new entity.

For information about the properties on each tab, see the following:

- See "General Entity Properties" on page 74 for information about specifying properties on the **General** tab.
- See "Contacts and Notification Entity Properties" on page 78 for information about specifying properties on the **Contacts/Notification** tab.
- See "Import Entity Properties" on page 79 for information about specifying properties on the **Import** tab.
- See "Display Entity Properties" on page 84 for information about specifying properties on the **Display** tab.

To change data group paths for all entities

- After you have logged in to the Administration Console as a global administrator, on the left pane, click **Entities**.
- Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Change Data Group Paths for All Entities**.
 - On the toolbar, click **Change Data Group Paths for All Entities**.
 - Right-click the selected item, and then click **Change Data Group Paths for All Entities**.
- In the **Select New Data Group Path for all Entities** dialog box, type or select the new data group path.
- In the **File Name** box, if you don't want to use the default value of **DGPATH**, then type a name for the path.
- Click **Save**.

**N O T E**

The changed path applies only to newly imported or created data groups. Existing data groups are not effected.

To find an entity ID

- After you have logged in to the Administration Console as a global administrator, on the left pane, click **Entities**.
- Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Find Entity ID**.
 - On the toolbar, click **Find Entity ID**.
 - Right-click the selected item, and then click **Find Entity ID**.

3. In the **Find Entity ID** dialog box, type the ID number for the entity, and then click **OK**.

If the system finds a matching entity ID, it selects it. If it does not find a match, a message appears stating the it was unable to locate the entity.

To refresh the list of entities

1. After you have logged in to the Administration Console as a global administrator, on the left pane, click **Entities**.
2. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Refresh**.
 - On the toolbar, click **Refresh**.
 - Right-click the selected item, and then click **Refresh**.

To delete an entity



I M P O R T A N T

Deleting an entity removes all traces of its existence from the database, and removes any full-text databases. However, whether document files are deleted from their storage media when the entity is deleted depends on whether the **Purge data groups during entity deletion** setting is selected. If selected, data groups that have a **Read/Write** state will be deleted from the storage media when the entity is deleted. Otherwise, document files are not erased. See "To set data processing items" on page 53 for instructions to specify the **Purge data groups during entity deletion** setting.

1. After you have logged in to the Administration Console as a global administrator, on the left pane, click **Entities**.
2. On the right pane, click the entity to delete, and then do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Delete**.
 - On the toolbar, click **Delete**.
 - Right-click the selected item, and then click **Delete**.
3. To proceed with the deletion, click **Yes**.

To set entity properties

1. After you have logged in to the Administration Console as a global administrator, on the left pane, click **Entities**.
2. On the right pane, click the entity, and then do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Properties**.
 - On the toolbar, click **Properties**.
 - Right-click the selected item, and then click **Properties**.
3. Click the tab that has the properties you want to edit. For information about the properties on each tab, see the following:
 - See "General Entity Properties" on page 74 for information about specifying properties on the **General** tab.

- See "Contacts and Notification Entity Properties" on page 78 for information about specifying properties on the **Contacts/Notification** tab.
- See "Import Entity Properties" on page 79 for information about specifying properties on the **Import** tab.
- See "Display Entity Properties" on page 84 for information about specifying properties on the **Display** tab.

To complete orphaned worksteps



NOTE

Orphaned worksteps are those that are unowned and uncompleted, but the associated workflow instance is completed. Performing the following procedure removes orphaned worksteps for the entity.

1. After you have logged in to the Administration Console as a global administrator, on the left pane, click **Entities**.
2. On the right pane, click the entity, and then do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Complete Orphaned Worksteps**.
 - On the toolbar, click **Complete Orphaned Worksteps**.
 - Right-click the selected item, and then click **Complete Orphaned Worksteps**.
3. To proceed, click **Yes**.

To verify/create database indexes



TIP

Performing the following procedure checks that all database tables, columns, stored procedures, and indexes exist, and if necessary creates them. This ensures that you can upgrade to the latest version of PaperVision Enterprise from any previous version.

1. After you have logged in to the Administration Console as a global administrator, on the left pane, click **Entities**.
2. On the right pane, click the entity, and then do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Verify/Create DB Indexes**.
 - Right-click the selected item, and then click **Verify/Create DB Indexes**.
3. To proceed, click **Yes**.

This page was intentionally inserted without content.



CHAPTER 4

Entity Administration

Setting Entity Properties	74
Backup Processing	87
Current Activity	91
Data Storage	97
General Security	135
Migration Jobs	149



Setting Entity Properties

Entity properties set system-level functions related to the entity. See "Entity" on page 22 for a brief functional overview and definition of an entity.

To access entity properties

1. After you have logged in to the Administration Console, on the left pane, click **Entities**.
2. On the right pane, click the entity to edit, and then do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Properties**.
 - On the toolbar, click **Properties**.
 - Right-click the selected item, and then click **Properties**.
3. In the **New Entity** dialog box, click the tab that has the properties you want to edit.

For information about the properties on each tab, see the following:

- See "General Entity Properties" below for instructions to set properties on the **General** tab.
- See "Contacts and Notification Entity Properties" on page 78 for instructions to set properties on the **Contacts/Notification** tab.
- See "Import Entity Properties" on page 79 for instructions to set properties on the **Import** tab.
- See "Display Entity Properties" on page 84 for instructions to set properties on the **Display** tab.

General Entity Properties

This content describes how to set the entity properties on the **General** tab. Each property is described in the following procedures.

To set the entity name

1. After you have logged in to the Administration Console, on the left pane, click **Entities**.
2. On the right pane, click the entity, and then do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Properties**.
 - On the toolbar, click **Properties**.
 - Right-click the selected item, and then click **Properties**.
3. Click the **General** tab.
4. In the **Entity Name** box, type a name for the company or organization.

To set database properties



IMPORTANT

Modifying these settings after an entity is created is necessary only when the database is moved or any of the following change: the database name, the name of the Windows server that hosts the database, or the user account used to access the database. If you change the settings to reference a new database, the system does not create the entity tables in the new database. This occurs only when a new entity is added. If you modify these settings, they must connect to an existing PaperVision Enterprise database that already has entity tables or else the entity will no longer function.

1. After you have logged in to the Administration Console, on the left pane, click **Entities**.
2. On the right pane, click the entity, and then do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Properties**.
 - On the toolbar, click **Properties**.
 - Right-click the selected item, and then click **Properties**.
3. Click the **General** tab.
4. In the **Database Settings** area, click **Configure**.
5. In the **SQL Data Source Information** dialog box, you can set the following items:
 - **Server IP/Name** - This setting specifies either the IP address or the machine name where the database resides.
 - **Database** - This setting specifies the database name used to share data with PaperVision Enterprise.
 - **User Name** - This setting specifies the user name for the person who has permissions to create new users and add new data. The default user name is derived from the System Administrator account specified when the SQL database was installed. If you do not want to use the System Administrator account, enter the name of a user that can be created automatically and granted the appropriate permissions in SQL server.
 - **Password** - This setting specifies the password for the user in the **User Name** box.
 - **Connection Type** - This setting specifies the connection type you want to use. If you select TCP/IP, then type the applicable port number in the **TCP/IP Port** box.
 - **TCP/IP Port** - This setting specifies port number for the TCP/IP connection.
6. Click **OK**.
7. If the **Attach to Existing Database Tables** check box is available, you can select it to cause the system to prompt for a new entity ID (instead of automatically generating one), and then use the existing database tables that have the provided entity ID in their name. Selecting this option is useful when the tables for an entity exist in a restored database that is separate from the PaperVision Enterprise system tables.

To set entity paths

1. After you have logged in to the Administration Console, on the left pane, click **Entities**.
2. On the right pane, click the entity, and then do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Properties**.
 - On the toolbar, click **Properties**.
 - Right-click the selected item, and then click **Properties**.
3. Click the **General** tab.

4. In the **Entity Paths** area, you can set the following items:



NOTE

The following paths do not need to be unique for an entity, nor amongst multiple entities. However, when PaperVision Enterprise takes a storage utilization snapshot, it evaluates the size of the entire contents of the data group, batch, and full-text paths separately. If any of these paths are identical, incorrect utilization calculations may occur, as the contents of the same directory are evaluated multiple times.

- **Data Group Path** - This setting specifies where imported data groups are copied and where new (attached) documents and new document versions are written. To set this path, do one of the following:
 - In the **Data Group Path** box, type the path.
 - Click the ellipsis button next to the **Data Group Path** box, select the path, and then click **Save**.
- **Migration/Backup Path** - This setting specifies the path where migration jobs or backup packages are processed. To set this path, do one of the following:
 - In the **Migration/Backup Path** box, type the path.
 - Click the ellipsis button next to the **Migration/Backup Path** box, select the path, and then click **Save**.
- **Full-Text Path** - This setting specifies the path where full-text database indexes are stored. To set this path, do one of the following:
 - In the **Full-Text Path** box, type the path.
 - Click the ellipsis button next to the **Full-Text Path** box, select the path, and then click **Save**.
- **Batch Path** - This setting specifies where batches created by the PaperVision Capture product are stored. To set this path, do one of the following:
 - In the **Batch Path** box, type the path.
 - Click the ellipsis button next to the **Batch Path** box, select the path, and then click **Save**.

To set migration job properties

1. After you have logged in to the Administration Console, on the left pane, click **Entities**.
2. On the right pane, click the entity, and then do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Properties**.
 - On the toolbar, click **Properties**.
 - Right-click the selected item, and then click **Properties**.
3. Click the **General** tab.
4. In the **Migration Jobs** area, you can set the following items:
 - **Max Data Group Size (MB)** - This setting specifies in megabytes the maximum size of data groups. The default setting is 2000.
 - **Max Documents per XML** - This setting specifies the maximum number of documents per XML data group. When this value is reached, separate XML files (within the same data group)

are created. To stop the creation of multiple-part XML data groups, set this value to zero. The default setting is 1000.

- **Notify Administrators** - When this option is selected, a notification is sent to administrators when migration jobs are complete. The notification includes the data groups that were created during the migration job.
- **Data Group Packaging** - To specify how data groups are packaged, select one of the following options:
 - **Uncompressed Data Groups** - Selecting this option creates uncompressed data groups in the PVE XML data group format.
 - **Zip Files** - Selecting this option compresses data groups into a zip file format. This setting is the default.
 - **Package Files** - Selecting this option compresses data groups into a package file format (file extension PVPKG) that can be imported directly into PaperVision Enterprise.

To disable the entity



NOTE

Disabling an entity prevents any users (including administrators) from logging in to PaperVision Enterprise.

1. After you have logged in to the Administration Console, on the left pane, click **Entities**.
2. On the right pane, click the entity, and then do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Properties**.
 - On the toolbar, click **Properties**.
 - Right-click the selected item, and then click **Properties**.
3. Click the **General** tab.
4. Near the bottom of the tab, select **Disable Entity**.

To disable utilization tracking



NOTE

By default, every user operation within PaperVision Enterprise is tracked so that administrators can perform security audits and run utilization reports. Selecting the **Disable Utilization Tracking** option turns this tracking off.

1. After you have logged in to the Administration Console, on the left pane, click **Entities**.
2. On the right pane, click the entity, and then do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Properties**.
 - On the toolbar, click **Properties**.
 - Right-click the selected item, and then click **Properties**.
3. Click the **General** tab.
4. Near the bottom of the tab, select **Disable Utilization Tracking**.

Contacts and Notification Entity Properties

This content describes how to set the entity properties on the **Contacts/Notification** tab. Each property is described in the following procedures.



NOTE

The contact information you specify is solely for reference purposes. There is no functionality associated with entering this information.

To add a technical contact

1. After you have logged in to the Administration Console, on the left pane, click **Entities**.
2. On the right pane, click the entity, and then do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Properties**.
 - On the toolbar, click **Properties**.
 - Right-click the selected item, and then click **Properties**.
3. Click the **Contacts/Notifications** tab.
4. In the **Technical Contact** area, type the name, phone number, and email address in the appropriate boxes.

To add a billing contact

1. After you have logged in to the Administration Console, on the left pane, click **Entities**.
2. On the right pane, click the entity, and then do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Properties**.
 - On the toolbar, click **Properties**.
 - Right-click the selected item, and then click **Properties**.
3. Click the **Contacts/Notifications** tab.
4. In the **Billing Contact** area, type the name, phone number, and email address in the appropriate boxes.

To set the notification method for users

1. After you have logged in to the Administration Console, on the left pane, click **Entities**.
2. On the right pane, click the entity, and then do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Properties**.
 - On the toolbar, click **Properties**.
 - Right-click the selected item, and then click **Properties**.
3. Click the **Contacts/Notifications** tab.
4. In the **Notification Method** area, select one of the following items:
 - **Publish Notification** - If selected, notifications are published in the database and accessed in the Administration Console and from PaperVision Enterprise when users click the down arrow next to their user name on the title bar, and then click **Notifications**.
 - **Send Email** - If selected, notifications are sent via email to the user's email address.

- **Publish Notification and Send Email** - If selected, notifications are published and sent via email as described in the previous two options.

Import Entity Properties

This content describes how to set the entity properties on the **Import** tab. Import properties define default settings for how data groups are imported. Each property is described in the following procedures.

To set the default import data group state

1. After you have logged in to the Administration Console, on the left pane, click **Entities**.
2. On the right pane, click the entity, and then do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Properties**.
 - On the toolbar, click **Properties**.
 - Right-click the selected item, and then click **Properties**.
3. Click the **Import** tab.
4. Under **Default Import Data Group State**, you can set the following items:
 - **Read-Only** - If selected, imported data groups are marked as read-only, and when a document is deleted, only the reference pointers to that document are deleted from the database. No files are deleted.
 - **Read/Write (Files can be deleted)** - If selected, imported data groups are marked as read/write, and when a document is deleted, the files are physically deleted from their source data group. To delete all documents in a data group, you must purge the data group.

To load COLD data and external documents into the full-text database



NOTE

The default setting loads COLD data and external documents (such as Microsoft Word files) into the full-text database when they are imported or added. This lets you perform full-text searches on the information.

1. After you have logged in to the Administration Console, on the left pane, click **Entities**.
2. On the right pane, click the entity, and then do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Properties**.
 - On the toolbar, click **Properties**.
 - Right-click the selected item, and then click **Properties**.
3. Click the **Import** tab.
4. In the **Load COLD data and external documents into full-text engine** check box, do one of the following:
 - To load COLD data and external documents (such as Microsoft Word files) into the full-text database when they are imported or added, select the check box.
 - To exclude COLD data and external documents (such as Microsoft Word files) from the full-text database when they are imported or added, clear the check box.

To keep data group database archives after import



NOTE

Keeping data group database archives after data groups are imported is the default setting. As a data group is imported, the data group database is copied with a date and time stamp and placed in the same directory where the data group resides. You can use these copies to revert to an earlier version of the data group database if it has been updated or appended by adding additional documents from another application.

1. After you have logged in to the Administration Console, on the left pane, click **Entities**.
2. On the right pane, click the entity, and then do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Properties**.
 - On the toolbar, click **Properties**.
 - Right-click the selected item, and then click **Properties**.
3. Click the **Import** tab.
4. In the **Keep data group database archives after import** check box, do one of the following:
 - To keep data group database archives after data groups are imported, select the check box.
 - To discard data group database archives after data groups are imported, clear the check box.

To set the default import type

1. After you have logged in to the Administration Console, on the left pane, click **Entities**.
2. On the right pane, click the entity, and then do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Properties**.
 - On the toolbar, click **Properties**.
 - Right-click the selected item, and then click **Properties**.
3. Click the **Import** tab.
4. Under **Default Import Type**, you can set the following items:
 - **Append** - If selected, only the new documents are added to an existing data group when you import the data group again.

- **Full/Reload** - If selected, all documents are overwritten in an existing data group when you import the data group again. Selecting this option does not delete documents that were deleted from the data group with another application. For all documents to be deleted from a data group, you must purge the data group. During a full/reload import, the document index values for existing documents are updated. After updating the index values, the system can either leave the document objects (page and pointers to document files) as they are, or you can select the **Apply object changes during reload** option and then choose a method for updating document objects. See **Apply object changes during reload** below for more information.

**NOTE**

The **Full/Reload** option does not apply to Report Management and Message Manager data groups, as these data groups support only append imports.

- **Delete Orphaned Documents** - This option is available only when **Full/Reload** is selected. If selected, during an import, the system compares the list of documents in the source data group against the list of documents in the PaperVision Enterprise database. If documents that no longer exist in the source data group are still present in the database, the system deletes them.

To set import error handling

**NOTE**

Data groups are validated during import to verify that all files and required index fields exist. You can specify to halt the import process if the data group fails validation. Choose from the options described in the following procedure.

1. After you have logged in to the Administration Console, on the left pane, click **Entities**.
2. On the right pane, click the entity, and then do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Properties**.
 - On the toolbar, click **Properties**.
 - Right-click the selected item, and then click **Properties**.
3. Click the **Import** tab.
4. Under **Import Error Handling**, you can set the following items:
 - **Halt import if missing files** - Select this option to stop the import of a data group if any of the files are missing.
 - **Halt import if missing required index fields** - Select this option to stop the import of a data group if any of the required index fields are missing.

To apply object changes during reload

1. After you have logged in to the Administration Console, on the left pane, click **Entities**.
2. On the right pane, click the entity, and then do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Properties**.
 - On the toolbar, click **Properties**.
 - Right-click the selected item, and then click **Properties**.
3. Click the **Import** tab.
4. To apply object changes during a reload, you can set the following items:
 - **Apply object changes during reload** - If selected, during a full/reload import, the document objects (pages and pointers to document files) are updated based on one of the following options. The options below are available only when you select this option.
 - **As new object version** - If selected, a new version of the object with updated page and pointer information from the data group is created. Any annotations applied to the imported documents are lost because this is a new version.
 - **As existing object version** - If selected, the existing version of the object is updated with the new page and pointer information from the data group. This ensures that any annotations that moved due to page insertions or deletions are placed into the appropriate location within the document. Using this option may increase the time needed to perform the import if a significant number of documents being imported were already annotated within PaperVision Enterprise.



CAUTION

For annotations in ScanTRAX™ Image and DataFlow™ COLD/ERM data group types, and multiple page TIFF files, the system cannot track how pages change in these file types. Therefore, annotations stay with the page number rather than following the image.

To set the default import copy settings

1. After you have logged in to the Administration Console, on the left pane, click **Entities**.
2. On the right pane, click the entity, and then do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Properties**.
 - On the toolbar, click **Properties**.
 - Right-click the selected item, and then click **Properties**.
3. Click the **Import** tab.

4. Under **Default Import Copy Settings**, you can set the following items:
 - **Copy data groups during import** - If selected, the entire contents of the data group is copied to a location in the data group path and then all documents are subsequently retrieved from that location. (See "To set entity paths" on page 75 for instructions to specify the data group path.)
 - **Delete source data group after copy** - This option is available only when **Copy data groups during import** is selected. If selected, after a data group is copied and the entire import is performed, the data group is deleted from its source location.

To send email validation reports after import

1. After you have logged in to the Administration Console, on the left pane, click **Entities**.
2. On the right pane, click the entity, and then do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Properties**.
 - On the toolbar, click **Properties**.
 - Right-click the selected item, and then click **Properties**.
3. Click the **Import** tab.
4. To send email validation reports after import, you can set the following items:
 - **Email validation reports after import** - During import, data groups are automatically validated to verify that all documents and required index fields exist. Select this option to send an email message (instead of the standard notification) to entity administrators, and then choose one of the following:
 - **Email administrators for failures only** - Select this option to send an email message with the validation information to entity administrators when a data group fails validation.
 - **Email administrators for both successes and failures** - Select this option to send an email message with the validation information to entity administrators when a data group is either validated successfully or fails validation.

To set data group auto-mapping

1. After you have logged in to the Administration Console, on the left pane, click **Entities**.
2. On the right pane, click the entity, and then do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Properties**.
 - On the toolbar, click **Properties**.
 - Right-click the selected item, and then click **Properties**.
3. Click the **Import** tab.
4. In the **Data group auto-mapping** area you can configure data groups exported from PaperVision Capture to automatically map to a specific entity.

These data groups contain a data group mapping file with the entity ID, and the mapping key encrypted data group name that must match the information in PaperVision Enterprise. If you specify a mapping key, any data group with a data group mapping file, must have a matching mapping key (data groups without a data group mapping file will be imported normally). You can also require that data groups must have a mapping file to be imported. Specify the following options to import data groups containing a data group mapping file.

- **Mapping Key** - Type an encryption key name that will be used to decrypt the data group when imported into PaperVision Enterprise, and used to encrypt the data group when exported from PaperVision Capture. This key ensures that only data groups that have been mapped by trusted sources are automatically imported into PaperVision Enterprise. This value must also be added to PaperVision Capture prior to exporting the data group. Please refer to the *PaperVision Capture Administration Guide* for more information on entering the mapping key value and entity information.
- **Require explicit mapping** - Select this option to import only data groups that contain a data group mapping file.

Display Entity Properties

This content describes how to set the entity properties on the **Display** tab. Display properties define default settings for how characters and document groupings appear, which method displays documents, and which file types are displayed. Each property is described in the following procedures.

To set the default character case display

1. After you have logged in to the Administration Console, on the left pane, click **Entities**.
2. On the right pane, click the entity, and then do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Properties**.
 - On the toolbar, click **Properties**.
 - Right-click the selected item, and then click **Properties**.
3. Click the **Display** tab.
4. For **Character Case Display**, you can select one of the following items:
 - **Upper Case Only** - If selected, all project names, index fields, and index values appear in uppercase letters.
 - **Mixed (Upper and Lower) Case** - If selected, all project names, index fields, and index values appear in uppercase and lowercase letters.

To set the default document grouping



NOTE

This setting specifies the default type of grouping applied to documents when they appear in search results. When document grouping is enabled from PaperVision Enterprise, (by clicking the down arrow next to the *user name* on the title bar, and then clicking **User Options**) the document grouping option specified there overrides this setting. When document grouping is selected, up to 100 documents with the same index values appear as if they were a single document. Document grouping is particularly useful when you want to continue to add pages to existing documents.

1. After you have logged in to the Administration Console, on the left pane, click **Entities**.
2. On the right pane, click the entity, and then do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Properties**.
 - On the toolbar, click **Properties**.
 - Right-click the selected item, and then click **Properties**.

3. Click the **Display** tab.
4. For **Default Document Grouping**, you can select one of the following items:
 - **None** - If selected, documents are not grouped. This is the default setting.
 - **Oldest First** - If selected, documents are grouped with the oldest documents at the beginning pages.
 - **Most Recent First** - If selected, documents are grouped with the newest documents at the beginning pages.

To set the default web document display method

1. After you have logged in to the Administration Console, on the left pane, click **Entities**.
2. On the right pane, click the entity, and then do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Properties**.
 - On the toolbar, click **Properties**.
 - Right-click the selected item, and then click **Properties**.
3. Click the **Display** tab.
4. Under **Default Web Document Display Method**, you can select one of the following items:
 - **Use PaperVision Viewer** - If selected, the PaperVision Viewer displays documents.
 - **Use Browser-Based Viewer** - If selected, the Browser-Based Viewer displays documents.



T I P

See “Select a Document Viewer” in the PaperVision Enterprise user guide or online help for information about the features of each viewer.

To display a notification when an upgraded document viewer is available

1. After you have logged in to the Administration Console, on the left pane, click **Entities**.
2. On the right pane, click the entity, and then do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Properties**.
 - On the toolbar, click **Properties**.
 - Right-click the selected item, and then click **Properties**.
3. Click the **Display** tab.
4. Select **Display Document Viewer Upgrade Availability** to cause a notification to appear for web users when they attempt to first view a document or workflow when a later version of the PaperVision Viewer is available.

To set file types to display in registered application



T I P

This function is particularly useful if you use proprietary file formats or file formats not supported by PaperVision Enterprise.

1. After you have logged in to the Administration Console, on the left pane, click **Entities**.
2. On the right pane, click the entity, and then do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Properties**.
 - On the toolbar, click **Properties**.
 - Right-click the selected item, and then click **Properties**.
3. Click the **Display** tab.
4. In the **File Types to Display in Registered Application** box, type the file types you want to appear in their native applications, regardless of which viewer is specified as the default. To specify multiple file extensions, separate them with the pipe character (|).



I M P O R T A N T

PaperVision Enterprise security settings do not apply to files opened in their native applications. For example, if users open PDF files in Adobe® Acrobat®, they can print those files, regardless of their assigned security rights within that PaperVision Enterprise project.

To set utilization report options

1. After you have logged in to the Administration Console, on the left pane, click **Entities**.
2. On the right pane, click the entity, and then do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Properties**.
 - On the toolbar, click **Properties**.
 - Right-click the selected item, and then click **Properties**.
3. Click the **Import** tab.
4. Under **Utilization Reports**, you can set the following items:
 - **Include Project Page Counts** - If selected, the utilization report calculates the number of pages in each project and includes this data in the report.
 - **Include User Usage Statistics** - If selected, the utilization report calculates usage statistics for each user and includes this data in the report.



N O T E

Selecting these options might increase the run time for utilization reports.

Backup Processing

Using backup processing, you can specify that certain information is backed up. When a backup job runs, it creates a package file that contains the backed up information. The package file uses compression that is 100% compatible with the existing PKZip 2.04g format and optional WinZip 9.0 AES encryption. Because the contents of the package is stored referentially, using an automated tool (such as the PaperVision Data Transfer Manager) to extract the content to a separate location lets you maintain a duplicate copy of all of the documents and full text data in a separate location from the original.

Backup package files may also include the following unencrypted files:

- **PackageCreationFailures.txt** - This file lists any files that were scheduled for back up, but could not be located during the backup job.
- **<Package File Name>.pvpkginfo** - This XML file contains the associated entity ID and the name (not the value) of the encryption key used to encrypt the package.

Before running backup jobs, ensure that:

- The **Migration/Backup Path** setting for the entity is specified. (See "To set entity paths" on page 75 for more information.)
- The **Package Workspace** setting is specified. (See "To configure local settings" on page 60 for more information.)
- The package file encryption key is specified if you want to encrypt the backup package files. (See "Encryption Keys" on page 135 for more information.)
- The **Backup Processing** operation is scheduled. (See "Configure Automation Service Scheduling" on page 61 for more information.)

For each backup job, you can select the projects to back up, the package file size and encryption key, and a schedule for running the backup job. The **Processing Logs** record information for each backup package file that is successfully created.



N O T E

Backup jobs back up only files and data in data groups and projects. To perform a complete system backup, you must also back up your SQL database.

To access backup processing options

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Backup Processing**.

For information about the items under **Backup Processing**, see the following:

- See "Backup Jobs" on the next page for the backup job tasks you can perform.
- See "Processing Logs" on page 90 for a description of the **Processing Logs** and the related tasks you can perform.

Backup Jobs

When a backup job runs, it creates a package file that contain the backed up information. (See "Backup Processing" on the previous page for more information about package files.) For each backup job, you can select the projects to back up, the package file size and encryption key, and a schedule for running the backup job. Each backup job option is described in the following procedures. In addition to the backup job types described in this section, you can also back up data groups and those jobs appear on the **Backup Jobs** pane. (See "Back Up Data Groups" on page 112 for instructions.)



NOTE

Backup jobs back up only files and data in data groups and projects. To perform a complete system backup, you must also back up your SQL database.

To view backup jobs

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Backup Processing**.
3. Click **Backup Jobs**.

The right pane shows for each backup job the:

- Name of the job
- Type of backup
- Schedule on which it runs
- Date and time for the next run time
- Date and time for the last run time
- Status of the job after the last run time

To add a backup job

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Backup Processing**.
3. Click **Backup Jobs**.
4. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **New Backup Job**.
 - On the toolbar, click **New**.
 - Right-click the selected item, and then click **New Backup Job**.
5. In the **Job Name** box, type a name for the backup job.
6. From the **Backup Type** list, select one of the following options:
 - **Backup Full Text** - If selected, the contents of the full text database is backed up for the projects you select
 - **Backup Project(s) - Full** - If selected, the full document contents (including all revisions) is backed up for the projects you select. When the next backup starts, the system resets the last document object backed up to zero, which forces the entire project to be backed up.

- **Backup Project(s) - Incremental** - If selected, the full document contents (including all revisions) is backed up for the projects you select. As the backup job for each project completes, the last document object that was backed up is recorded so that when the next backup job occurs, the system will start where it left off.
7. Under **Projects to Backup**, select the projects to be backed up by this job.
 8. In the **Max. Package Contents (MB)** box, type the maximum size in MB of the content data that is placed into a backup package. When this size is reached, a new package file is created.

**N O T E**

This value does not specify the size of the package file itself, but the size of its contents before compression. This value can be overwritten by the **Max. Backup Package Contents Size (MB)** global system setting. (See "To set options for data size management" on page 54 for information about this global setting.)

9. To encrypt the backup package files, from the **Package File Encryption Key** list, select the encryption key.
10. Click the **Schedule** tab, and in the **Start Time** box, type the date and time for the backup job to start running.

By default, this box displays the date and time when you began adding the backup job. (See "Date and Time Format Information" on page 23 if you need help understanding the correct date and time format to use.)
11. To set a schedule for the backup job, from the **Schedule** list, select the unit of time on which to base the schedule.
12. In the **Repeat Every** box, specify the frequency of repetition for the operation.
13. Click **OK** to add the new backup job.

To refresh the list of backup jobs

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Backup Processing**.
3. Click **Backup Jobs**.
4. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Refresh**.
 - On the toolbar, click **Refresh**.
 - Right-click the selected item, and then click **Refresh**.

To delete backup jobs

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Backup Processing**.
3. Click **Backup Jobs**.

4. On the right pane, select the backup job(s) to delete (hold down the Ctrl key to select multiple items), and then do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Delete**.
 - On the toolbar, click **Delete**.
 - Right-click the selected item, and then click **Delete**.
5. To confirm the deletion, click **Yes**.

To edit the properties of a backup job

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Backup Processing**.
3. Click **Backup Jobs**.
4. On the right pane, select the backup job, and then do one of the following:
 - Double-click the selected item.
 - On the **Action** menu, point to **All Tasks**, and then click **Properties**.
 - On the toolbar, click **Properties**.
 - Right-click the selected item, and then click **Properties**.
5. On the **Backup Job Properties** dialog box, you can make changes to the backup job. (See "To add a backup job" on page 88 for information about setting each backup job property.) Your changes will take effect the next time the backup job is run.

Processing Logs

The **Processing Logs** record each time a backup package file was successfully created. This information lets you review how much data is being backed up each time a back up job runs. (See "Backup Processing" on page 87 and "Backup Jobs" on page 88 for more information about backup jobs.)

To view the Processing Logs

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Backup Processing**.
3. Click **Processing Logs**.

The right pane shows for each backup job the:

- Name of the backup job
- Date and time of the last run time
- Size of the backup file in MB
- Type of information that was backed up

To refresh the Processing Logs

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Backup Processing**.
3. Click **Processing Logs**.

4. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Refresh**.
 - On the toolbar, click **Refresh**.
 - Right-click the selected item, and then click **Refresh**.

Current Activity

Under **Current Activity**, you can access functions to manage user sessions, document grants, and locked user accounts. In addition, you can access notifications about system events that might need your attention.

To access current activity options

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Current Activity**.

For information about the items under **Current Activity**, see the following:

- See "Current Sessions" below for a description of current session information and the related tasks you can perform.
- See "Document Grants" on page 93 for a description of how document grants work and the related tasks you can perform.
- See "Locked Users" on page 94 for a description of the tasks you can perform for locked users.
- See "Notifications at the Entity Level" on page 95 for a description of notifications and the related tasks you can perform.

Current Sessions

Each time a user logs in to PaperVision Enterprise a session is started. Every time a user accesses the server, the system verifies that the session is still valid, performs the requested operation, and then records the date and time of the last activity. If a user session is idle for too long (as specified by the administrator), the session may be automatically terminated. Automatically terminating a session logs the user out of the system. This feature is useful for releasing licenses that are unnecessarily being used, for example, a user went to lunch without logging out, or the application was closed without the user logging out.

The following settings determine when user sessions are automatically terminated:

- **Client Ping Increment** - This is a global setting that must be specified by a global administrator. This setting specifies the interval in seconds between each “ping” the client application sends to the server. When a user logs in, if their client application can ping the server, the server instructs it to do so at the interval specified here. This background ping verifies that the client application is open and keeps the user session active. If a client has not sent the expected ping within 60 seconds of the specified ping interval, the session is automatically terminated. Without ping validation, the user session does not terminate until the session times out as specified by the **Max Session Idle Time** setting described below. (See “To set the client ping increment” on page 52 for instructions to set this value.)



NOTE

Because some mobile browsers do not support background operations, the **Client Ping Increment** setting does not apply to Android and iPad devices. For these devices, the **Max Session Idle Time** setting for the entity determines the length of the user session.

- **Max Global Session Idle Time** - This is a global setting that must be specified by a global administrator. This setting specifies the maximum number of minutes that a user session can remain idle before the automation service automatically logs the user out of the system. (See “To set utilization limits” on page 51 for instructions to set this value.)
- **Max Session Idle Time** - This is an entity setting and specifies the maximum number of minutes that a user session can be inactive before it is automatically terminated. (See “To set the maximum session idle time” on page 138 for instructions to set this value)



NOTE

If the maximum session idle time is set at both the global and entity level, the global setting determines the maximum value and the entity setting determines what the value is. The value of the entity setting cannot exceed the value of the global setting.

To view the current user sessions

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Current Activity**.
3. Click **Current Sessions**.

The right pane shows for each active user session the:

- Name of the user
- Date and time the user logged in
- Date and time the user’s last activity occurred
- Date and time the last ping was sent
- Licenses being used by the user

To kill current user sessions

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Current Activity**.
3. Click **Current Sessions**.
4. Select the user session(s) to kill (hold down the Ctrl key to select multiple items).
5. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Kill**.
 - On the toolbar, click **Kill**.
 - Right-click the selected item, and then click **Kill**.

To refresh the list of current user sessions

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Current Activity**.
3. Click **Current Sessions**.
4. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Refresh**.
 - On the toolbar, click **Refresh**.
 - Right-click the selected item, and then click **Refresh**.

Document Grants

A document grant provides direct access to a document within PaperVision Enterprise via a web-based URL. This feature eliminates the need to fax documents or send them as email attachments, and reduces security risks.

User rights to create document grants are assigned by the entity administrator at the project level. (See "Add Project Security Access" on page 188 for instructions.) When a document grant is created, the user can set an expiration date and password for it. Although document grants expire, you can also manually delete them, as described under "To delete document grants" on the next page. Multiple document grants can be created for the same document.

To view the active document grants

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Current Activity**.
3. Click **Document Grants**.

The right pane shows for each document grant the:

- Name of the user who issued the grant
- Date and time the grant was created
- Name of the project that contains the document grant
- Date and time the document grant expires
- Document to which the grant provides access

To delete document grants

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Current Activity**.
3. Click **Document Grants**.
4. Select the document grant(s) to delete (hold down the Ctrl key to select multiple items).
5. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Delete**.
 - On the toolbar, click **Delete**.
 - Right-click the selected item, and then click **Delete**.

To refresh the list of active document grants

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Current Activity**.
3. Click **Document Grants**.
4. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Refresh**.
 - On the toolbar, click **Refresh**.
 - Right-click the selected item, and then click **Refresh**.

Locked Users

The account lockout security policy assigned to the entity determines whether user accounts get locked by the system, how many invalid login attempts can occur before a user account is locked, and whether the locked account and the lockout counters are automatically reset after a specified number of minutes. (See "Account Lockout Security Policy" on page 140 for more information.) Even if the account lockout security policy is set to automatically unlock a locked account after a specified number of minutes, you can manually unlock the account before the specified time has elapsed.

To view locked users

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Current Activity**.
3. Click **Locked Users**.

The right pane shows for each locked user the:

- Name of the user
- Date and time the account lock occurred
- Location where the account lock occurred

To unlock a locked user

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Current Activity**.
3. Click **Locked Users**.
4. Select the user(s) to unlock (hold down the Ctrl key to select multiple items).

5. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Unlock**.
 - On the toolbar, click **Unlock**.
 - Right-click the selected item, and then click **Unlock**.
6. On the confirmation message, click **Yes** to unlock the user.

To refresh the list of locked users

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Current Activity**.
3. Click **Locked Users**.
4. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Refresh**.
 - On the toolbar, click **Refresh**.
 - Right-click the selected item, and then click **Refresh**.

Notifications at the Entity Level

Notifications are messages that are usually generated and sent by the system when events occur that may need your attention. You can also manually send notifications to system users. Whether notifications are created manually or by the system, global notifications are sent only to global accounts and entity notifications are sent only to entity accounts. (See "Notifications at the Global Level" on page 47 for information about how global notifications work.) Entity users can access their notifications in PaperVision Enterprise by clicking their user name on the title bar, and then clicking **Notifications**.

Entity notifications are sent using the notification method specified in the properties for the entity. (See "To set the notification method for users" on page 78 for instructions.)

As an entity administrator, you receive automated notifications when:

- a data group is successfully loaded
- a migration job is processing
- a migration job is complete (if configured to do so)
- attempts to log in occur on a locked account
- attempts to log in occur when all licenses are in use
- the source IP address or host name changed in the middle of a session (if the security policy prohibits this)

An entity user receives notifications when:

- an entity administrator manually sends them
- a workstep instance remains unprocessed for too long and the user is part of a user group defined for that workflow

To view entity notifications

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Current Activity**.

3. Click **Notifications**.

The right pane shows the date and time the notification was sent, and the recipient and source of the notification.

To create a new notification

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Current Activity**.
3. Click **Notifications**.
4. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **New Notification**.
 - On the toolbar, click **New**.
 - Right-click the selected item, and then click **New Notification**.
5. In the **New Notification** dialog box, from the **Recipient** list, select the person to receive the notification.
6. In the **Message** box, type the message to send, and then click **OK**.

To refresh the list of notifications

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Current Activity**.
3. Click **Notifications**.
4. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Refresh**.
 - On the toolbar, click **Refresh**.
 - Right-click the selected item, and then click **Refresh**.

To delete notifications

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Current Activity**.
3. Click **Notifications**.
4. Select the notification(s) to delete (hold down the Ctrl key to select multiple items), and then do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Delete**.
 - On the toolbar, click **Delete**.
 - Right-click the selected item, and then click **Delete**.
5. Click **Yes** to confirm the deletion.

To view the properties of a notification

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Current Activity**.
3. Click **Notifications**.

4. On the right pane, click the notification, and then do one of the following:
 - Double-click the notification.
 - On the **Action** menu, point to **All Tasks**, and then click **Properties**.
 - On the toolbar, click **Properties**.
 - Right-click the selected item, and then click **Properties**.

Data Storage

Under **Data Storage**, you can access functions to manage data groups and the file sets that are appended to data groups.

To access data storage options

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Data Storage**.

For information about the items under **Data Storage**, see the following:

- See "Data Groups" below for the definition of a data group and instructions to access the data group functions you can perform.
- See "Message Capture File Sets" on page 119 for a description of Message Capture file sets and the related tasks you can perform.
- See "Report Management File Sets" on page 127 for a description of Report Management file sets and the related tasks you can perform.

Data Groups

A data group is a set of documents and their index values. A data group can contain one or thousands of documents, and those documents can be grouped into one or many projects. A data group holds information specific to a single entity, but it can contain an unlimited number of projects. Typically, a data group contains only documents for one project, as this makes organization easier. You can import data groups from many different sources. (See "Data Group Types for Import" on page 105 for more information.)

To access data group functions

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Data Storage**.
3. On the right pane, click **Data Groups**. Do one of the following:
 - Double-click the selected item.
 - On the **Action** menu, point to **All Tasks**, and then click **Data Groups**.
 - On the toolbar, click **Data Groups**.
 - Right-click the selected item, and then click **Data Groups**.

The **Data Groups** window shows a list of imported data groups and shows for each data group the:

- Unique name for the data group assigned by the system
- Type of data group

- Size of the data group in megabytes
- Read/Write state of the data group
- Date and time that the data group was last updated
- Project to which the data group was imported (the last loaded document ID appears in parentheses after the project name)
- Path to which the data group was imported
- Original data group name assigned by the originating program
- Encryption state of the data group



NOTE

Data groups that are in the Recycle Bin display with a red background. (See "Restore Data Groups from the Recycle Bin" on page 116 and "Empty Data Groups from the Recycle Bin" on page 115 for more information.)

4. (Optional) In the **Max Items** box, you can type the maximum number of data groups to appear in the list, and then on the toolbar click **Refresh**.

As you work with data groups, see the following related sections for additional information.

- See "Filter the Data Groups List" on the facing page for instructions to complete this task.
- See "Refresh the Data Groups List" on page 100 for instructions to complete this task.
- See "Print the Data Groups List" on page 100 for instructions to complete this task.
- See "Create New Attachment Data Groups" on page 101 for instructions to complete this task.
- See "Import Data Groups" on page 101 for instructions to complete this task.
- See "Data Group Types for Import" on page 105 for a list of data group types you can import.
- See "Modify Data Group Paths" on page 108 for instructions to complete this task.
- See "Resize Data Groups" on page 108 for instructions to complete this task.
- See "Move Data Groups" on page 109 for instructions to complete this task.
- See "Encrypt and Decrypt Data Groups" on page 110 for instructions to complete this task.
- See "Migrate Data Groups" on page 112 for instructions to complete this task.
- See "Back Up Data Groups" on page 112 for instructions to complete this task.
- See "Validate Data Groups" on page 113 for instructions to complete this task.
- See "Change the Read/Write State for All Data Groups" on page 114 for instructions to complete this task.
- See "Empty Data Groups from the Recycle Bin" on page 115 for instructions to complete this task.
- See "Restore Data Groups from the Recycle Bin" on page 116 for instructions to complete this task.
- See "Purge Data Groups" on page 117 for instructions to complete this task.
- See "Edit Data Group Properties" on page 118 for instructions to complete this task.

Filter the Data Groups List

To find specific data groups more easily, you can apply filter criteria to the list of data groups.

To filter the data groups list

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Data Storage**.
3. On the right pane, click **Data Groups**. Do one of the following:
 - Double-click the selected item.
 - On the **Action** menu, point to **All Tasks**, and then click **Data Groups**.
 - On the toolbar, click **Data Groups**.
 - Right-click the selected item, and then click **Data Groups**.
4. Do one of the following:
 - On the **Action** menu, click **Filter**.
 - On the toolbar, click **Filter**.
5. In the **Data Storage Filter** dialog box, you can specify the following filter criteria:
 - In the **Name** box, type the system-assigned name for the data group.
 - In the **Type** list, select the data group type.
 - In the **Last Imported** boxes, type the date range for data group imports in the **YYYY-MM-DD hh:mm:ss** format . (See "Date and Time Format Information" on page 23 for more information.)
 - In the **Project** list, select the project.
 - In the **Original Name** box, type the original data group name assigned by the originating program.
6. Click **OK**.



NOTE

Below the listed results, the number of items displayed appears followed by **(Filtered)** to indicate that a filter is applied to the data groups list.

To remove a filter from the data groups list

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Data Storage**.
3. On the right pane, click **Data Groups**. Do one of the following:
 - Double-click the selected item.
 - On the **Action** menu, point to **All Tasks**, and then click **Data Groups**.
 - On the toolbar, click **Data Groups**.
 - Right-click the selected item, and then click **Data Groups**.

4. Do one of the following:
 - On the **Action** menu, click **Filter**.
 - On the toolbar, click **Filter**.
5. In the **Data Storage Filter** dialog box, click **Clear Filter**, and then click **OK**.

Refresh the Data Groups List

To ensure the data groups list contains the most current information, you can manually refresh it.

To refresh the data groups list

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Data Storage**.
3. On the right pane, click **Data Groups**. Do one of the following:
 - Double-click the selected item.
 - On the **Action** menu, point to **All Tasks**, and then click **Data Groups**.
 - On the toolbar, click **Data Groups**.
 - Right-click the selected item, and then click **Data Groups**.
4. Do one of the following:
 - On the **Action** menu, click **Refresh**.
 - On the toolbar, click **Refresh**.

Print the Data Groups List

You can print the list of data groups as it appears on the **Data Groups** window.

To print the data groups list

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Data Storage**.
3. On the right pane, click **Data Groups**, and then do one of the following:
 - Double-click the selected item.
 - On the **Action** menu, point to **All Tasks**, and then click **Data Groups**.
 - On the toolbar, click **Data Groups**.
 - Right-click the selected item, and then click **Data Groups**.
4. On the **Data Groups** window, do one of the following:
 - On the **Action** menu, click **Print**.
 - On the toolbar, click **Print**.
5. In the **Print** dialog box, specify the print options, and then click **OK**.

Create New Attachment Data Groups

As you attach or add new documents or check in a new document version, the new files are automatically placed into an attachment data group. If an attachment data group does not already exist, it is automatically created. After an attachment data group is created, all new attachments for that project are placed into this new data group. In some cases, this data group can become quite large, and you might want to create a new attachment data group in a different storage location. All attached documents and new document versions are always placed into the most recently created attachment data group for that project.

To create a new attachment data group

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Data Storage**.
3. On the right pane, click **Data Groups**. Do one of the following:
 - Double-click the selected item.
 - On the **Action** menu, point to **All Tasks**, and then click **Data Groups**.
 - On the toolbar, click **Data Groups**.
 - Right-click the selected item, and then click **Data Groups**.
4. Do one of the following:
 - On the **Action** menu, point to **Data Groups**, and then click **Create New Attachment Data Group**.
 - On the toolbar, click **Create New Attachment Data Group**.
 - Right-click the data group list, and then click **Create New Attachment Data Group**.
5. Read the message that appears, and then click **Yes** to continue.
 The new attachment data group appears in the data group list with a name of **ATTACH** followed by the date you created it.

Import Data Groups

You can import data groups from multiple sources. (See "Data Group Types for Import" on page 105 for a list of data group source types and their file extensions.) The default import options are set in the properties for the entity (as described under "Import Entity Properties" on page 79), but you can override them when you manually import data groups.

When a data group is imported (with the exception of C.A.R. data groups), the system checks if the necessary projects already exist and creates them if they are not present. The system then compares the index field names in the data group with the index field names in the existing project.

EXAMPLE

The following project index fields already exist:

- Account Number
- Customer Name
- Invoice Date

When the following data group index fields are imported:

- Customer Name - The index value will populate the second index field in the existing Customer Name project index field.
- Account Number - The index value will populate the first index field in the existing Account Number project index field.
- PO Number - The index value will be ignored because this field does not exist in the project (but could be added manually).

Because the data group does not contain an Invoice Date index field, the existing Invoice Date project index field will populate with a value of [Blank].



NOTE

When importing PaperFlow data groups with projects that contain the tilde ("~") character, PaperVision Enterprise recognizes only the portion of the project name to the left of the tilde. This lets PaperFlow users create multiple projects that contain the same index field setup, but have different scan, process, and index location settings, and then have those projects imported into the same PaperVision Enterprise project.

As data groups are imported, after the documents for a project are ingested, the system attempts to apply document security levels and create WorkFlow instances (per applicable pre-conditions), and import any full-text data for those documents. Any uncompleted process is automatically added as a maintenance queue item, allowing the remainder of the data group to be imported successfully. (See "Maintenance Queue" on page 44 for more information.)

To import a data group

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Data Storage**.
3. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Data Groups**.
 - On the toolbar, click **Data Groups**.
 - Right-click the selected item, and then click **Data Groups**.

4. On the **Data Groups** window, do one of the following:
 - On the **Action** menu, point to **Data Groups**, and then click **Import Data Group**.
 - On the toolbar, click **Import Data Group**.
5. In the **Import New Data Group** dialog box, do one of the following:
 - In the **Path** box, type the path to the data group to import.
 - Click the ellipsis button, select the path to the data group to import, and then click **Open**.
(See "Data Group Types for Import" on page 105 for a list of data group source types and their file extensions.)

**NOTE**

If you use a UNC path, any automation server can import the data group. Otherwise, only the current automation server can perform the import.

6. In the **Import Method** area, select one of the following items:
 - **Submit Job to be Imported Automatically** - If selected, the system places the item on the **Import Queue** for the automation service to process. (See "Configure Automation Service Scheduling" on page 61 and "Import Queue" on page 34 for more information.)
 - **Import Immediately** - If selected, the system immediately imports the data group. If you select this option, you must wait for the import to complete before you can do anything else in the Administration Console.
 - **Map Data Group to Entity** - If selected, the system maps the data group information to the entity so that any data groups that the automation service identifies that have the same customer ID and name will automatically be imported into the entity. If the data group is for a new project, this mapping must exist. Selecting this option does not immediately import the data group, but the mapping is created so that the automation service knows where to put the data group when it imports it in the background, so you don't have to wait for the import to complete. For automatic imports to occur, you must have the automation service configured to do so. (See "Configure Automation Service Scheduling" on page 61 and "Import Queue" on page 34 for more information.)
7. In the **Import Type** area, select one of the following items:
 - **Append** - If selected, only the new documents are added to an existing data group when you import the data group again.

- **Full/Reload** - If selected, all documents are overwritten in an existing data group when you import the data group again. Selecting this option does not delete documents that were deleted from the data group with another application. (For all documents to be deleted from a data group, you must purge the data group. (See "Purge Data Groups" on page 117 for instructions.) During a full/reload import, the document index values for existing documents are updated. After updating the index values, the system can either leave the document objects (page and pointers to document files) as they are, or you can select the **Apply object changes during reload** option and then choose a method for updating document objects. See **Apply object changes during reload** in the next step for more information.



N O T E

The **Full/Reload** option does not apply to data groups that were never imported, as new data groups are always imported as an append import type. In addition, PaperVision Enterprise Report Management (PVERM) and PaperVision Message Capture Manager (PVMSG) data groups support only append imports.

- **Delete Orphaned Documents** - This option is available only when **Full/Reload** is selected. If selected, during an import, the system compares the list of documents in the source data group against the list of documents in the PaperVision Enterprise database. If documents that no longer exist in the source data group are still present in the database, the system deletes them.
8. If you selected **Full/Reload** for the import type, you can set the following options:
- **Apply object changes during reload** - If selected, during a full/reload import, the document objects (pages and pointers to document files) are updated based on one of the following options.
 - **As new object version** - If selected, a new version of the object with updated page and pointer information from the data group is created. Any annotations applied to the imported documents are lost because this is a new version.
 - **As existing object version** - If selected, the existing version of the object is updated with the new page and pointer information from the data group. With the exception of the ScanTRAX™ Image and DataFlow™ COLD/ERM data group types, and multiple page TIFF files, any annotations that moved due to page insertions or deletions are placed into the appropriate location within the document. Using this option may increase the time needed to perform the import if a significant number of documents being imported were already annotated within PaperVision Enterprise.
9. Under **Import Copy Settings**, you can set the following items:
- **Copy data groups during import** - If selected, the entire contents of the data group is copied to a location in the data group path and then all documents are subsequently retrieved from that location. See "To set entity paths" on page 75 for instructions to set the
 - **Delete source data group after copy** - This option is available only when **Copy data groups during import** is selected. If selected, after a data group is copied and the entire import is performed, the data group is deleted from its source location.

10. Depending on the import method you selected, do one of the following
- Click **Submit** to place the data group on the **Import Queue** for the automation service to process.
 - Click **Start** to immediately import the data group.
 - Click **Map** to create mapping for the data group.

Data Group Types for Import

You can import data groups from the sources in the following table. All data groups are produced by their respective applications, with the exception of C.A.R. and XML formatted data groups. If you are working with these data groups types, see "About C.A.R. Data Groups" below and "About XML Data Groups" on the next page for additional information.

Data Group Source	File Extension
Digitech Systems' PaperFlow™ Image Data Group Format	DATAGRP.MDB
Digitech Systems' DataFlow™ COLD/ERM Data Group Format	COLDGRP.DAT
Digitech Systems' PaperVision Enterprise Report Management Data Group Format	ERMGROUP.XML
Digitech Systems' PaperVision Message Capture Data Group Format	MSGGROUP.XML
Digitech Systems' PaperVision Package File Format (See "PaperVision Package Files" on the next page for more information.)	PVPKG
ImageMax's Docu-ROM™ Image Data Group Format	CDSTAMP.MDB
ImageMax's ScanTRAX™ Image Data Group Format	PROJECT.MDB
C.A.R. (film-based) Formatted Text File	CARFILE.TXT
XML Formatted Data Group	DATAGRP.XML

About C.A.R. Data Groups

Computer Aided Retrieval (C.A.R.) allows users to search through film-based images and digital documents in data groups. When a user selects a document that is stored on film, the user is notified and given the roll and frame number where the image is located. PaperVision Enterprise imports C.A.R. files that are "pipe-delimited text files." These text files contain the index information and the roll and frame number on which to locate a document.

EXAMPLE

For example, you can load the following sample C.A.R. file into PaperVision Enterprise.

[CAR]

DGNAME=99990001

DEPTNAME=ABC Corporation

PROJNAME=Accounts Payable

ACME CORP. | 12/31/98 | 19421 | 1

B SQUARE | 12/30/98 | 19421 | 4

When working with C.A.R. files, keep the following in mind:

- The first four lines of the C.A.R. file should always be formatted as shown above.
- The **DGNAME** value specifies the unique identifier given to this C.A.R. data group. No other C.A.R. data group should ever have the same **DGNAME** value unless you are adding data to an existing data group.
- The **DEPTNAME** value should contain the department or company name to which the data group belongs.
- The **PROJNAME** field contains the name of an existing project in PaperVision Enterprise into which the documents will be imported. Unlike all of the other import data group formats supported by PaperVision Enterprise, C.A.R. data groups are the only type that require the project to already be specified.
- PaperVision Enterprise will import the index field data based on the order of the index fields. The index fields are given, followed by a roll number, then a frame number. You must supply all index fields defined in a project. If specific information for a field is not available, you can leave the value blank, but be sure to leave a placeholder for the information.

About XML Data Groups

PaperVision Enterprise supports importing XML-formatted data groups. This lets you import documents of any type (images, Microsoft Word, PDF files, etc.) from any application capable of creating XML files. The format required for an XML data group is specified in the **DATAGRP Format.XML** file located in the **\Digitech Systems\PaperVision\Docs** directory where PaperVision Enterprise was installed.

PaperVision Package Files

PaperVision Package Files are compressed and optionally encrypted files that contain all of the files (in the appropriate directory structure) for one of the supported data group types and include a file extension of **PVPKG**. (See "Data Group Types for Import" on the previous page for a list of supported data group types.)

Package files are particularly useful when you need to:

- transport a data group with added security by using encryption.
- increase file transfer speeds by transferring one large file rather than hundreds or thousands of small files.

Package files use compression and optional encryption that are 100% compatible with the PKZIP 2.04g compression format and the WinZip 9.0 AES encryption format. Therefore, package files can be created using most popular ZIP compression tools. However, you can use the PaperVision Data Transfer Manager to completely automate the creation and transport of package files.

To import package files, they must include a package information file. This file is an additional unencrypted file embedded in the root of the package file.

- The name of the package information file is: ***PackageFileName.pvpkginfo***
- The contents of the file are:

```
<?xml version="1.0"?>
<PVPACKAGEINFO>
  <ENTID>EntityIDHere</ENTID>
  <ENCRYPTKEYNAME>KeyNameHere</ENCRYPTKEYNAME>
  <IMPORTFILE>ImportFileNameHere</IMPORTFILE>
</PVPACKAGEINFO>
```

As PaperVision Enterprise imports a package file, it follows this process:

1. PaperVision Enterprise extracts the package information file.
2. It determines if the package contents are encrypted by checking the **ENTID** and **ENCRYPTKEYNAME** values.
3. If **ENCRYPTKEYNAME** has a value, it retrieves the encryption key value that corresponds to the encryption key name and entity ID, and uses it to decrypt the remaining contents of the package.
4. The contents of the package file are extracted to the **Package Workspace** path defined under your global system settings. (See "Local System Settings" on page 60 for more information.)
5. After the contents of the file are fully extracted, it uses the file name specified in **IMPORTFILE**, to determine the data group type, and then imports the data group.
6. After the import is complete, it removes the package file contents from the **Package Workspace** path.

Modify Data Group Paths

If data groups are moved to a new location, you must modify the specified data group path that the system uses to find them. You can modify the path for a single data group, or select multiple data groups to modify their paths at the same time. When you select multiple data groups, the system evaluates their paths and finds their common path.



NOTE

If you move data groups using the **Submit for Move** command on the **Data Groups** window, the system automatically updates the path to point to the new location that is specified in the entity properties. (See "Move Data Groups" on the facing page for more information.)

To modify data group paths

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Data Storage**.
3. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Data Groups**.
 - On the toolbar, click **Data Groups**.
 - Right-click the selected item, and then click **Data Groups**.
4. On the **Data Groups** window, select the data group(s) for path modification (hold down the Ctrl key to select multiple items).
5. Do one of the following:
 - Right-click the selected data group(s), and then click **Modify Path**.
 - On the **Action** menu, point to **Data Groups**, and then click **Modify Path**.
 - On the toolbar, click **Modify Path**.
6. In the **Search and Replace Path** dialog box, do one of the following:
 - In the **Replacement Path** box, type the new replacement path for the selected data group(s).
 - Click the ellipsis button, select the new replacement path for the selected data group(s), and then click **Save**.
7. Click **Replace**.

Resize Data Groups

When you resize a data group, the system recalculates the total space used by each of the files within the data group. If this amount is less than the space recorded in the database, a notification is sent to all global administrators to inform them of the discrepancy. The discrepancy might indicate that the data path was accessed outside of PaperVision Enterprise and that data has been moved, changed, or deleted.

To resize data groups

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Data Storage**.

3. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Data Groups**.
 - On the toolbar, click **Data Groups**.
 - Right-click the selected item, and then click **Data Groups**.
4. On the **Data Groups** window, select the data group(s) to resize (hold down the Ctrl key to select multiple items).
5. Do one of the following:
 - On the **Action** menu, point to **Data Groups**, and then click **Resize**.
 - On the toolbar, click **Resize**.
 - Right-click the selected item(s), and then click **Resize**.
6. In the **Resize Data Group** dialog box, click **Yes**.

Move Data Groups

You can move data groups to the data group path specified for an entity. This feature is useful when storage limits are exceeded and data must be moved to other storage options. During data groups moves the system:

1. Copies the entire contents of the data group to the new data group path specified in the properties for the entity. (See "Modify Data Group Paths" on the previous page for instructions)
2. Updates the recorded location of the data group in the database.
3. Attempts to delete the original data group from its source location.

This process ensures that the data group remains available for access during the entire move process. The data group move appears as an item on the Maintenance Queue to be processed by the automation service. (See "Maintenance Queue" on page 44 and "Configure Automation Service Scheduling" on page 61 for more information.)



NOTE

During data group moves, the system ignores data groups that already exist in the new data group path and In-Line data groups (that is, those that are only referenced in their current location by directory).



IMPORTANT

Do not import the data group at the same time that you attempt to move it.

To move data groups



NOTE

Before performing this procedure, ensure that the data group path for the entity is set to the location where you want to move the data groups. See "To set entity paths" on page 75 for more information.

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Data Storage**.
3. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Data Groups**.
 - On the toolbar, click **Data Groups**.
 - Right-click the selected item, and then click **Data Groups**.
4. On the **Data Groups** window, select the data group(s) to move (hold down the Ctrl key to select multiple items).
5. Do one of the following:
 - On the **Action** menu, point to **Data Groups**, and then click **Submit for Move**.
 - On the toolbar, click **Submit for Move**.
 - Right-click the selected item(s), and then click **Submit for Move**.
6. In the **Submit Data Group Move** dialog box, click **Yes**.

The appropriate maintenance queue items are created to be processed by the automation service when it is scheduled to do so.

Encrypt and Decrypt Data Groups

As data groups are imported or documents are added, they can be encrypted to ensure the data is secure while stored. When an encrypted document is requested, the data is automatically decrypted for display. Encryption is not available for the following data group types:

- **In-Line** data groups cannot be encrypted because they are not managed by PaperVision Enterprise. They are created by directory manager jobs that are not configured to copy the files to a data group.
- Digitech Systems' PaperVision Enterprise Report Management COLD Data Group Format does not support encryption at the data group level. However, you can apply encryption to the data as it is processed by selecting the **File Set Encryption Key** option in the Report Management Job configuration. (See "To set general options for a Report Management Job" on page 229 for instructions.)
- Digitech Systems' PaperVision Message Capture Data Group Format does not support encryption at the data group level. However, you can apply encryption to the data as it is processed by selecting the **Message Encryption Key** in the message capture policy set configuration. (See "To specify file set options" on page 215 for instructions.)
- Digitech Systems' DataFlow™ COLD/ERM Data Group Format does not support encryption at the data group level because accessing a single page of a very large report file requires decrypting the entire file.

For data groups that were imported without encryption, you can add it, and you can decrypt data groups that were imported with encryption. When a data group is submitted for encryption or decryption, a maintenance job is created and placed on the **Maintenance Queue** for the automation service to process. (See "Maintenance Queue" on page 44 for more information.) During encryption, the data group is copied (while encrypted) to a secondary location. This lets users access the data group during the encryption process. After the encryption is complete, the reference to the data group is updated to point to the newly encrypted location. The old, unencrypted directory is then submitted as a deletion job for the automation service to process.

**N O T E**

Before you can encrypt data groups, you must ensure that the:

Encryption key is added. (See "Encryption Keys" on page 135 for instructions.)

Security Policy for the entity is configured to support data group encryption. (See "To assign encryption keys" on page 139 for instructions.)

Data groups submitted for encryption are marked as **Read/Write**. (See "Change the Read/Write State for All Data Groups" on page 114 for instructions.)

To submit data groups for encryption

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Data Storage**.
3. On the right pane, click **Data Groups**. Do one of the following:
 - Double-click the selected item.
 - On the **Action** menu, point to **All Tasks**, and then click **Data Groups**.
 - On the toolbar, click **Data Groups**.
 - Right-click the selected item, and then click **Data Groups**.
4. On the **Data Groups** window, select the data group(s) to submit for encryption (hold down the Ctrl key to select multiple items).
5. Do one of the following:
 - On the **Action** menu, point to **Data Groups**, and then click **Submit for Encryption**.
 - On the toolbar, click **Submit for Encryption**.
 - Right-click the selected item(s), and then click **Submit for Encryption**.
6. Click **Yes** to confirm the submission, and then click **OK**.

To submit data groups for decryption

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Data Storage**.
3. On the right pane, click **Data Groups**. Do one of the following:
 - Double-click the selected item.
 - On the **Action** menu, point to **All Tasks**, and then click **Data Groups**.

- On the toolbar, click **Data Groups**.
 - Right-click the selected item, and then click **Data Groups**.
4. On the **Data Groups** window, select the data group(s) to submit for decryption (hold down the Ctrl key to select multiple items).
 5. Do one of the following:
 - On the **Action** menu, point to **Data Groups**, and then click **Submit for Decryption**.
 - On the toolbar, click **Submit for Decryption**.
 - Right-click the selected item(s), and then click **Submit for Decryption**.
 6. Click **Yes** to confirm the submission, and then click **OK**.

Migrate Data Groups

When you migrate a data group, it is copied and then formatted into an XML data group. (See "Migration Jobs" on page 149 for more information.)

To migrate data groups

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Data Storage**.
3. On the right pane, click **Data Groups**. Do one of the following:
 - Double-click the selected item.
 - On the **Action** menu, point to **All Tasks**, and then click **Data Groups**.
 - On the toolbar, click **Data Groups**.
 - Right-click the selected item, and then click **Data Groups**.
4. On the **Data Groups** window, select the data group(s) to submit for migration (hold down the Ctrl key to select multiple items).
5. Do one of the following:
 - On the **Action** menu, point to **Data Groups**, and then click **Submit for Migration**.
 - On the toolbar, click **Submit for Migration**.
 - Right-click the selected item(s), and then click **Submit for Migration**.
6. Click **Yes** to confirm the migration operation.

Back Up Data Groups

You can submit a data group to be backed up in its entirety. Data group back up jobs are initially scheduled to run only once, but you can modify the properties of backup jobs after they are submitted and appear on the **Backup Jobs** pane. (See "Backup Processing" on page 87 to learn about how backups work and "Backup Jobs" on page 88 for options you can specify for backup jobs on the **Backup Jobs** pane.)

To back up data groups

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Data Storage**.

3. On the right pane, click **Data Groups**. Do one of the following:
 - Double-click the selected item.
 - On the **Action** menu, point to **All Tasks**, and then click **Data Groups**.
 - On the toolbar, click **Data Groups**.
 - Right-click the selected item, and then click **Data Groups**.
4. On the **Data Groups** window, select the data group(s) to submit for back up (hold down the Ctrl key to select multiple items).
5. Do one of the following:
 - On the **Action** menu, point to **Data Groups**, and then click **Submit for Backup**.
 - On the toolbar, click **Submit for Backup**.
 - Right-click the selected item(s), and then click **Submit for Backup**.
6. Click **Yes** to confirm the backup operation.
7. From the **Backup Package Encryption Key** list, select either the correct encryption key or **<No Encryption/Decryption Used>**.
8. Click **OK** to confirm the backup operation.

Validate Data Groups

Entity administrators can submit data groups to be queued for validation. During the validation process, the range of imported documents is checked to ensure that all files for each document exist.

When data groups are submitted for validation, they appear on the **Maintenance Queue** to be purged by the automation service. (See "Configure Automation Service Scheduling" on page 61 and "Maintenance Queue" on page 44 for more information.)

To submit selected data groups for validation

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Data Storage**.
3. On the right pane, click **Data Groups**. Do one of the following:
 - Double-click the selected item.
 - On the **Action** menu, point to **All Tasks**, and then click **Data Groups**.
 - On the toolbar, click **Data Groups**.
 - Right-click the selected item, and then click **Data Groups**.
4. On the **Data Groups** window, select the data group(s) to submit for validation (hold down the Ctrl key to select multiple items).
5. Do one of the following:
 - On the **Action** menu, point to **Data Groups**, and then click **Submit for Validation**.
 - On the toolbar, click **Submit for Validation**.
 - Right-click the data group list, and then click **Submit for Validation**.
6. Click **Yes** to confirm the validation.

To submit all listed data groups for validation

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Data Storage**.
3. On the right pane, click **Data Groups**. Do one of the following:
 - Double-click the selected item.
 - On the **Action** menu, point to **All Tasks**, and then click **Data Groups**.
 - On the toolbar, click **Data Groups**.
 - Right-click the selected item, and then click **Data Groups**.
4. Do one of the following:
 - On the **Action** menu, point to **Data Groups**, and then click **Submit All for Validation**.
 - On the toolbar, click **Submit All for Validation**.
 - Right-click the data group list, and then click **Submit All for Validation**.
5. Click **Yes** to confirm the validation.

Change the Read/Write State for All Data Groups

The Read/Write state of data groups affects how information is handled when data groups are purged.

- When data groups in a **Read/Write** state are purged (and the project does not recycle documents), the actual data files are deleted from their storage location, along with the index values and reference pointers stored in the database. This information can not be restored.
- When data groups in a **Read Only** state are purged (and the project does not recycle documents), only the index values and reference pointers stored in the database are deleted. No actual data files are deleted, unless the **Force purged data group deletion** option is selected. (See "Purge Data Groups" on page 117 for more information.)

Use the following procedure to change the Read/Write state for all listed data groups at the same time. See "Edit Data Group Properties" on page 118 for instructions to modify the Read/Write state for a single data group at a time.

To change the Read/Write state for all listed data groups

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Data Storage**.
3. On the right pane, click **Data Groups**. Do one of the following:
 - Double-click the selected item.
 - On the **Action** menu, point to **All Tasks**, and then click **Data Groups**.
 - On the toolbar, click **Data Groups**.
 - Right-click the selected item, and then click **Data Groups**.

4. Do one of the following:
 - On the **Action** menu, point to **Data Groups**, and then click **Change Read/Write for All Data Groups**.
 - On the toolbar, click **Change Read/Write for All Data Groups**.
 - Right-click the data group list, and then click **Change Read/Write for All Data Groups**.
5. Select either **Read-Only** or **Read/Write**, and then click **OK**.
6. Click **Yes** to confirm the setting.

Empty Data Groups from the Recycle Bin

Whether data groups appear in the Recycle Bin after they are purged depends on the Recycle Bin settings for the project. (See "Edit Project Properties" on page 162 for instructions to set Recycle Bin options.) Data groups that are in the Recycle Bin display with a red background. You can view the date and time it was recycled and by whom in the data group properties. (See "Edit Data Group Properties" on page 118 for instructions to open data group properties.) The date and time is recorded when the data group is initially purged, and it is not updated. For example, if you purge a data group, its properties show the date and time it was sent to the Recycle Bin. If you later select all data groups, and then purge them, the original date and time of the previously purged data group is not updated.

What happens to data when you empty the Recycle Bin depends on the Read/Write state of the data group and how your global administrator set the **Force purged data group deletion** option. Before emptying the Recycle Bin, review how the following items affect the data.

- When data groups in a **Read/Write** state are emptied from the Recycle Bin, the actual data files are deleted from their storage location, along with the index values and reference pointers stored in the database. This information can not be restored. (See "Edit Data Group Properties" on page 118 to change the Read/Write state of a single data group or "Change the Read/Write State for All Data Groups" on the previous page to change the Read/Write state for all data groups.)
- When data groups in a **Read Only** state are emptied from the Recycle Bin, only the index values and reference pointers stored in the database are deleted. No actual data files are deleted, unless the **Force purged data group deletion** option (described below) is selected.
- If your global administrator selected the **Force purged data group deletion** option, when a data group is emptied from the Recycle Bin, the files are always removed from the storage media, regardless of the Read/Write state of the data group. (See "To set data processing items" on page 53 for instructions to change this option.)



C A U T I O N

Use caution when emptying data groups in a Read/Write state from the Recycle Bin, as you may permanently delete data.

Use caution when emptying In-Line data groups in a Read/Write state from the Recycle Bin. These are simply directories that were imported via the directory manager. Because the directory manager may not have imported all of the files in these In-Line data groups, or the directories may be used for other purposes, emptying them may cause undesired results.

To empty data groups from the Recycle Bin

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Data Storage**.
3. On the right pane, click **Data Groups**. Do one of the following:
 - Double-click the selected item.
 - On the **Action** menu, point to **All Tasks**, and then click **Data Groups**.
 - On the toolbar, click **Data Groups**.
 - Right-click the selected item, and then click **Data Groups**.
4. On the **Data Groups** window, select the recycled data group(s) to empty from the Recycle Bin (hold down the Ctrl key to select multiple items).
5. Do one of the following:
 - On the **Action** menu, point to **Data Groups**, and then click **Empty from Recycle Bin**.
 - Right-click the selected item(s), and then click **Empty from Recycle Bin**.
6. Read the message that appears, and then select one of the following items:
 - **Submit Empty Job** - If selected, the system places the data group(s) on the **Maintenance Queue** for the automation service to process. (See "Configure Automation Service Scheduling" on page 61 and "Maintenance Queue" on page 44 for more information.)
 - **Empty Immediately** - If selected, the system immediately empties the data group(s) from the Recycle Bin.



C A U T I O N

If the selected data group(s) are in a **Read Only** state, they are immediately emptied from the Recycle Bin regardless of which option you select.

7. To proceed, click **Empty**, and then click **Yes** to confirm the empty operation.

Restore Data Groups from the Recycle Bin

Whether data groups appear in the Recycle Bin after they are purged depends on the Recycle Bin settings for the project. (See "Edit Project Properties" on page 162 for instructions to set Recycle Bin options.) Data groups that are in the Recycle Bin display with a red background. You can view the date and time it was recycled and by whom in the data group properties. (See "Edit Data Group Properties" on page 118 for instructions to open data group properties.)

To restore data groups from the Recycle Bin

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Data Storage**.
3. On the right pane, click **Data Groups**. Do one of the following:
 - Double-click the selected item.
 - On the **Action** menu, point to **All Tasks**, and then click **Data Groups**.
 - On the toolbar, click **Data Groups**.
 - Right-click the selected item, and then click **Data Groups**.

4. On the **Data Groups** window, select the recycled data group(s) to restore from the Recycle Bin (hold down the Ctrl key to select multiple items).
5. Do one of the following:
 - On the **Action** menu, point to **Data Groups**, and then click **Restore from Recycle Bin**.
 - Right-click the selected item(s), and then click **Restore from Recycle Bin**.
6. Click **Yes** to confirm the restore operation.

Purge Data Groups

When data groups are submitted to be purged, they appear on the **Deletion Queue** to be purged by the automation service. (See "Configure Automation Service Scheduling" on page 61 and "Deletion Queue" on page 29 for more information.)

Purging a data group deletes data it contains. How the deletion of data is handled during the purge process depends on the Read/Write state of the data group, project Recycle Bin settings, and how your global administrator set the **Force purged data group deletion** option. Before purging data groups, review how the following items affect the purge process.

- Project Recycle Bin settings determine whether documents are permanently deleted or placed in the Recycle Bin when they are purged. If a data group contains multiple projects, the Recycle Bin settings for those projects must be the same, or you will not be able to purge the data group. (See "Edit Project Properties" on page 162 for instructions to set Recycle Bin options.)
- When data groups in a **Read/Write** state are purged (and the project does not recycle documents), the actual data files are deleted from their storage location, along with the index values and reference pointers stored in the database. This information can not be restored. (See "Edit Data Group Properties" on the next page to change the Read/Write state of a single data group and "Change the Read/Write State for All Data Groups" on page 114 to change the Read/Write state for all data groups.)
- When data groups in a **Read Only** state are purged (and the project does not recycle documents), only the index values and reference pointers stored in the database are deleted. No actual data files are deleted, unless the **Force purged data group deletion** option (described below) is selected.
- If your global administrator selected the **Force purged data group deletion** option, when a data group is purged, the files are always removed from the storage media, regardless of the Read/Write state of the data group. (See "To set data processing items" on page 53 for instructions to change this option.)



CAUTION

Use caution when purging data groups in a Read/Write state, as you may permanently delete data.

Use caution when purging In-Line data groups in a Read/Write state. These are simply directories that were imported via the directory manager. Because the directory manager may not have imported all of the files in these In-Line data groups, or the directories may be used for other purposes, purging them may cause undesired results.

To purge data groups

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Data Storage**.
3. On the right pane, click **Data Groups**. Do one of the following:
 - Double-click the selected item.
 - On the **Action** menu, point to **All Tasks**, and then click **Data Groups**.
 - On the toolbar, click **Data Groups**.
 - Right-click the selected item, and then click **Data Groups**.
4. On the **Data Groups** window, select the data group(s) to purge (hold down the Ctrl key to select multiple items).
5. Do one of the following:
 - On the **Action** menu, point to **Data Groups**, and then click **Purge**.
 - On the toolbar, click **Purge**.
 - Right-click the selected item(s), and then click **Purge**.
6. Read the message that appears, and then select one of the following items:
 - **Submit Purge Job** - If selected, the system places the data group(s) on the **Deletion Queue** for the automation service to process. (See "Configure Automation Service Scheduling" on page 61 and "Deletion Queue" on page 29 for more information.)
 - **Purge Immediately** - If selected, the system immediately purges the data group(s). If you select this option, you must wait for the purge to complete before you can do anything else in the Administration Console.
7. To proceed, click **Purge**, and then click **Yes** to confirm the purge operation.

Edit Data Group Properties

Data group properties display the following information

- Unique name for the data group assigned by the system
- Date and time that the data group was last updated
- Type of data group
- Size of the data group in megabytes and kilobytes
- Encryption state of the data group
- Original data group name assigned by the originating program
- Path to which the data group was imported
- Project to which the data group was imported (the last loaded document ID appears in parentheses after the project name)
- Read/Write state of the data group
- For a recycled data group, the date and time it was recycled and by whom appear in red text. The date and time stamp is recorded when the data group is initially purged and it is not updated. For example, if you purge a data group, its properties show the date and time it was sent to the

Recycle Bin. If you later select all data groups, and then purge them, the date and time stamp of the previously deleted data group is not updated.

The Read/Write state of the data group is the only property you can change, and affects how information is handled when data groups are purged.

- When data groups in a **Read/Write** state are purged (and the project does not recycle documents), the actual data files are deleted from their storage location, along with the index values and reference pointers stored in the database. This information can not be restored.
- When data groups in a **Read Only** state are purged (and the project does not recycle documents), only the index values and reference pointers stored in the database are deleted. No actual data files are deleted, unless the **Force purged data group deletion** option is selected. (See "Purge Data Groups" on page 117 for more information.)

To edit data group properties

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Data Storage**.
3. On the right pane, click **Data Groups**. Do one of the following:
 - Double-click the selected item.
 - On the **Action** menu, point to **All Tasks**, and then click **Data Groups**.
 - On the toolbar, click **Data Groups**.
 - Right-click the selected item, and then click **Data Groups**.
4. On the **Data Groups** window, select the data group.
5. Do one of the following:
 - On the **Action** menu, point to **Data Groups**, and then click **Properties**.
 - On the toolbar, click **Properties**.
 - Right-click the selected item, and then click **Properties**.
6. To change the Read/Write state of the data group, select or clear the **Read/Write** check box.
7. Click **OK** to save the state of the data group.

Message Capture File Sets

The PaperVision Message Manager product processes email messages to prepare them for storage in PaperVision Enterprise. As email messages are processed, they are parsed into manageable pieces of data called Message Capture File Sets that are appended to data groups. Message Capture File Sets are specific to each entity. Message Capture File Sets are imported using the same process for importing data groups. (See "Import Data Groups" on page 101 for instructions.)

See "Message Manager Overview" on page 210 to access information about the contents of Message Capture File Sets and configuration options for them. Use the following procedure to access functions you can perform for the Message Capture File Sets that are already in the system.

To access functions for Message Capture File Sets

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Data Storage**.

3. On the right pane, click **Message Capture File Sets**. Do one of the following:
 - Double-click the selected item.
 - On the **Action** menu, point to **All Tasks**, and then click **Message Capture File Sets**.
 - On the toolbar, click **Message Capture File Sets**.
 - Right-click the selected item, and then click **Message Capture File Sets**.

The **Message Capture File Sets** window shows a list of imported Message Capture File Sets and shows for each one the:

- Date and time that the Message Capture File Set was last updated
- Unique name for the Message Capture File Set assigned by the system
- Name of the policy set used to create the Message Capture File Set and its ID number
- Workstation on which the automation service processed the data for the Message Capture File Set
- Data group to which the Message Capture File Set was appended
- Number of documents contained in the Message Capture File Set
- Number of messages contained in the Message Capture File Set
- Size of the Message Capture File Set in bytes
- Number of seconds it took to process the data used to create the Message Capture File Set



N O T E

Message Capture File Sets that are in the Recycle Bin display with a red background. (See "Restore Message Capture File Sets from the Recycle Bin" on page 125 and "Empty Message Capture File Sets from the Recycle Bin" on page 124 for more information.)

4. (Optional) In the **Max Items** box on the lower-right corner of the window, you can type the maximum number of data groups to appear in the list, and then on the toolbar click **Refresh**.

See "Message Manager Overview" on page 210 to access information about the contents of Message Capture File Sets and configuration options for them. See the following related sections for tasks you can perform for the Message Capture File Sets that are already in the system.

- See "Filter the Message Capture File Sets List" on the facing page for instructions to complete this task.
- See "Refresh the Message Capture File Sets List" on page 122 for instructions to complete this task.
- See "Print the Message Capture File Sets List" on page 122 for instructions to complete this task.
- See "Roll Back Message Capture File Sets" on page 123 for instructions to complete this task.
- See "Export Message Capture File Sets" on page 124 for instructions to complete this task.
- See "Empty Message Capture File Sets from the Recycle Bin" on page 124 for a list of data group types you can import.

- See "Restore Message Capture File Sets from the Recycle Bin" on page 125 for instructions to complete this task.
- See "View Message Capture File Sets Properties" on page 126 for instructions to complete this task.

Filter the Message Capture File Sets List

To find specific Message Capture File Sets more easily, you can apply filter criteria to the list of Message Capture File Sets.

To filter the Message Capture File Sets list

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Data Storage**.
3. On the right pane, click **Message Capture File Sets**. Do one of the following:
 - Double-click the selected item.
 - On the **Action** menu, point to **All Tasks**, and then click **Message Capture File Sets**.
 - On the toolbar, click **Message Capture File Sets**.
 - Right-click the selected item, and then click **Message Capture File Sets**.
4. Do one of the following:
 - On the **Action** menu, click **Filter**.
 - On the toolbar, click **Filter**.
5. In the **Data Storage Filter** dialog box, you can specify the following filter criteria:
 - In the **File Set Name** box, type the system-assigned name for the Message Capture File Set.
 - In the **Finished** boxes, type the date range for when updates occurred to the Message Capture File Set in the **YYYY-MM-DD hh:nn:ss** format. (See "Date and Time Format Information" on page 23 for more information.)
 - In the **Policy Set** box, type the name of the policy set used to create the Message Capture File Set.
 - In the **Data Group** box, type the original data group name to which the Message Capture File Set was appended.
6. Click **OK**.



NOTE

Below the listed results, the number of items displayed appears followed by **(Filtered)** to indicate that a filter is applied to the Message Capture File Sets List.

To remove a filter from the Message Capture File Sets list

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Data Storage**.

3. On the right pane, click **Message Capture File Sets**. Do one of the following:
 - Double-click the selected item.
 - On the **Action** menu, point to **All Tasks**, and then click **Message Capture File Sets**.
 - On the toolbar, click **Message Capture File Sets**.
 - Right-click the selected item, and then click **Message Capture File Sets**.
4. Do one of the following:
 - On the **Action** menu, click **Filter**.
 - On the toolbar, click **Filter**.
5. In the **Data Storage Filter** dialog box, click **Clear Filter**, and then click **OK**.

Refresh the Message Capture File Sets List

To ensure the Message Capture File Sets list contains the most current information, you can manually refresh it.

To refresh the Message Capture File Sets list

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Data Storage**.
3. On the right pane, click **Message Capture File Sets**. Do one of the following:
 - Double-click the selected item.
 - On the **Action** menu, point to **All Tasks**, and then click **Message Capture File Sets**.
 - On the toolbar, click **Message Capture File Sets**.
 - Right-click the selected item, and then click **Message Capture File Sets**.
4. Do one of the following:
 - On the **Action** menu, click **Refresh**.
 - On the toolbar, click **Refresh**.

Print the Message Capture File Sets List

You can print the list of Message Capture File Sets as it appears on the **Message Capture File Sets** window.

To print the Message Capture File Sets list

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Data Storage**.
3. On the right pane, click **Message Capture File Sets**, and then do one of the following:
 - Double-click the selected item.
 - On the **Action** menu, point to **All Tasks**, and then click **Message Capture File Sets**.
 - On the toolbar, click **Message Capture File Sets**.
 - Right-click the selected item, and then click **Message Capture File Sets**.

4. On the **Message Capture File Sets** window, do one of the following:
 - On the **Action** menu, click **Print**.
 - On the toolbar, click **Print**.
5. In the **Print** dialog box, specify the print options, and then click **OK**.

Roll Back Message Capture File Sets

Rolling back a Message Capture File Set deletes data it contains. This function is useful to remove Message Capture File Sets created by an incorrectly-configured job without affecting the rest of the information in the data group. How the deletion of data is handled during the roll back process depends on the Read/Write state of the data group to which the Message Capture File Set is appended and project Recycle Bin settings. Before rolling back Message Capture File sets, review how the following items affect the roll back process.

- Project Recycle Bin settings determine whether Message Capture File Sets are permanently deleted or placed in the Recycle Bin when they are rolled back. If the data groups to which the Message Capture File Sets are appended contain multiple projects, the Recycle Bin settings for those projects must be the same, or you will not be able to roll back the Message Capture File Sets. (See "Edit Project Properties" on page 162 for instructions to set Recycle Bin options.)
- If the data groups to which the Message Capture File Sets are appended are in a **Read/Write** state, when you roll back the Message Capture File Sets (and the project does not recycle documents), the actual data files are deleted from their storage location, along with the index values and reference pointers stored in the database. This information can not be restored. (See "Edit Data Group Properties" on page 118 to change the Read/Write state of a single data group and "Change the Read/Write State for All Data Groups" on page 114 to change the Read/Write state for all data groups.)
- If the data groups to which the Message Capture File Sets are appended are in a **Read Only** state, when you roll back the Message Capture File Sets (and the project does not recycle documents), only the index values and reference pointers stored in the database are deleted. No actual data files are deleted.



C A U T I O N

Use caution when rolling back Message Capture File Sets that are appended to data groups in a Read/Write state, as you may permanently delete data.

To roll back Message Capture File Sets

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Data Storage**.
3. On the right pane, click **Message Capture File Sets**. Do one of the following:
 - Double-click the selected item.
 - On the **Action** menu, point to **All Tasks**, and then click **Message Capture File Sets**.
 - On the toolbar, click **Message Capture File Sets**.
 - Right-click the selected item, and then click **Message Capture File Sets**.

4. On the **Message Capture File Sets** window, select the Message Capture File Set(s) to roll back (hold down the Ctrl key to select multiple items).
5. Do one of the following:
 - On the **Action** menu, point to **File Sets**, and then click **Roll Back**.
 - On the toolbar, click **Roll Back**.
 - Right-click the selected item(s), and then click **Roll Back**.
6. Read the message that appears, and if you want to proceed, click **Yes** to confirm the roll back operation.

Export Message Capture File Sets

You can export Message Capture File Sets into an XML file.

To export Message Capture File Sets

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Data Storage**.
3. On the right pane, click **Message Capture File Sets**, and then do one of the following:
 - Double-click the selected item.
 - On the **Action** menu, point to **All Tasks**, and then click **Message Capture File Sets**.
 - On the toolbar, click **Message Capture File Sets**.
 - Right-click the selected item, and then click **Message Capture File Sets**.
4. On the **Message Capture File Sets** window, select the Message Capture File Set(s) to export (hold down the Ctrl key to select multiple items).
5. Do one of the following:
 - On the **Action** menu, point to **File Sets**, and then click **Export**.
 - On the toolbar, click **Export**.
6. On the confirmation message, click **Yes**.
7. In the **Export File Set Entries** dialog box, select the location where the export file will go.
8. In the **File name** box, type a name for the export file, and then click **Save**.

Empty Message Capture File Sets from the Recycle Bin

Whether Message Capture File Sets appear in the Recycle Bin after they are rolled back depends on the Recycle Bin settings for the project. (See "Edit Project Properties" on page 162 for instructions to set Recycle Bin options.) Message Capture File Sets that are in the Recycle Bin display with a red background. You can view the date and time it was recycled and by whom in the Message Capture File Sets properties. (See "View Message Capture File Sets Properties" on page 126 for instructions to open Message Capture File Sets properties.)

The date and time is recorded when the Message Capture File Set is initially rolled back, and it is not updated. For example, if you roll back a Message Capture File Set, its properties show the date and time it was sent to the Recycle Bin. If you later select all Message Capture Files Sets, and then roll them back, the original date and time of the previously rolled back Message Capture File Set is not updated.

What happens to Message Capture File Set data when you empty the Recycle Bin depends on the Read/Write state of the data group to which it is appended. Before emptying the Recycle Bin, review how the following items affect the data.

- If the data groups to which the Message Capture File Sets are appended are in a **Read/Write** state, when you empty the Recycle Bin, the actual data files are deleted from their storage location, along with the index values and reference pointers stored in the database. This information can not be restored. (See "Edit Data Group Properties" on page 118 to change the Read/Write state of a single data group and "Change the Read/Write State for All Data Groups" on page 114 to change the Read/Write state for all data groups.)
- If the data groups to which the Message Capture File Sets are appended are in a **Read Only** state, when you empty the Recycle Bin, only the index values and reference pointers stored in the database are deleted. No actual data files are deleted.



C A U T I O N

Use caution when emptying Message Capture File Sets that are appended to data groups in a Read/Write state from the Recycle Bin, as you may permanently delete data.

To empty Message Capture File Sets from the Recycle Bin

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Data Storage**.
3. On the right pane, click **Message Capture File Sets**. Do one of the following:
 - Double-click the selected item.
 - On the **Action** menu, point to **All Tasks**, and then click **Message Capture File Sets**.
 - On the toolbar, click **Message Capture File Sets**.
 - Right-click the selected item, and then click **Message Capture File Sets**.
4. On the **Message Capture File Sets** window, select the recycled Message Capture File Set(s) to empty from the Recycle Bin (hold down the Ctrl key to select multiple items).
5. Do one of the following:
 - On the **Action** menu, point to **File Sets**, and then click **Empty from Recycle Bin**.
 - Right-click the selected item(s), and then click **Empty from Recycle Bin**.
6. Read the message that appears, and if you want to proceed, click **Yes** to confirm the empty operation.

Restore Message Capture File Sets from the Recycle Bin

Whether Message Capture File Sets appear in the Recycle Bin after they are rolled back depends on the Recycle Bin settings for the project. (See "Edit Project Properties" on page 162 for instructions to set Recycle Bin options.) Message Capture File Sets that are in the Recycle Bin display with a red background. You can view the date and time it was recycled and by whom in the Message Capture File Sets properties. (See "View Message Capture File Sets Properties" on the next page for instructions to open Message Capture File Sets properties.)

To restore Message Capture File Sets from the Recycle Bin

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Data Storage**.
3. On the right pane, click **Message Capture File Sets**. Do one of the following:
 - Double-click the selected item.
 - On the **Action** menu, point to **All Tasks**, and then click **Message Capture File Sets**.
 - On the toolbar, click **Message Capture File Sets**.
 - Right-click the selected item, and then click **Message Capture File Sets**.
4. On the **Message Capture File Sets** window, select the recycled Message Capture File Set(s) to restore from the Recycle Bin (hold down the Ctrl key to select multiple items).
5. Do one of the following:
 - On the **Action** menu, point to **File Sets**, and then click **Restore from Recycle Bin**.
 - Right-click the selected item(s), and then click **Restore from Recycle Bin**.
6. Click **Yes** to confirm the restore operation.

View Message Capture File Sets Properties

The properties for Message Capture File Sets display the following information:

- Start Date and time that the Message Capture File Set was created
- Finish Date and time that the Message Capture File Set was last updated
- Name of the policy set used to create the Message Capture File Set and its ID number
- Workstation on which the automation service processed the data for the Message Capture File Set
- Data group to which the Message Capture File Set was appended
- Data group file set identifier assigned by the system
- Number of documents contained in the Message Capture File Set
- Number of messages contained in the Message Capture File Set
- Size of the Message Capture File Set in bytes
- Number of seconds it took to process the data used to create the Message Capture File Set
- For a recycled Message Capture File Set, the date and time it was recycled and by whom appear in red text. The date and time stamp is recorded when the Message Capture File Set is initially rolled back, and it is not updated. For example, if you roll back a Message Capture File Set, its properties show the date and time it was sent to the Recycle Bin. If you later select all Message Capture File Sets, and then roll them back, the date and time stamp of the previously rolled back Message Capture File Set is not updated.

To view properties for Message Capture File Sets

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Data Storage**.

3. On the right pane, click **Message Capture File Sets**. Do one of the following:
 - Double-click the selected item.
 - On the **Action** menu, point to **All Tasks**, and then click **Message Capture File Sets**.
 - On the toolbar, click **Message Capture File Sets**.
 - Right-click the selected item, and then click **Message Capture File Sets**.
4. On the **Message Capture File Sets** window, select the Message Capture File Set.
5. Do one of the following:
 - Double-click the selected item.
 - On the **Action** menu, point to **File Sets**, and then click **Properties**.
 - On the toolbar, click **Properties**.
 - Right-click the selected item, and then click **Properties**.
6. When you are finished viewing the properties, click **Close**.

Report Management File Sets

The PaperVision Enterprise Report Management product performs COLD/ERM processing on print streams to prepare them for storage in PaperVision Enterprise. As the information is processed, it is parsed into manageable pieces of data called "Report Management File Sets" that are appended to data groups. Report Management File Sets are specific to each entity. Report Management File Sets can be imported using the same process for importing data groups or by a configured Report Management Job. (See "Import Data Groups" on page 101 and "Report Management Jobs" on page 225 for more information.)

See "Report Management Overview" on page 224 for access to information about the contents of Report Management File Sets and configuration options for Report Management Jobs. Use the following procedure to access functions you can perform for the Report Management File Sets that are already in the system.

To access functions for Report Management File Sets

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Data Storage**.
3. On the right pane, click **Report Management File Sets**. Do one of the following:
 - Double-click the selected item.
 - On the **Action** menu, point to **All Tasks**, and then click **Report Management File Sets**.
 - On the toolbar, click **Report Management File Sets**.
 - Right-click the selected item, and then click **Report Management File Sets**.

The **Report Management File Sets** window shows a list of imported Report Management File Sets and shows for each one the:

- Date and time that the Report Management File Set was last updated
- Unique name for the Report Management File Set assigned by the system
- Name of the Report Management Job that processed the Report Management File Set

- Workstation on which the automation service processed the data for the Report Management File Set
- Data group to which the Report Management File Set was appended
- Imported state of the Report Management File Set
- Number of documents contained in the Report Management File Set
- Number of pages contained in the Report Management File Set
- Size of the Report Management File Set in bytes
- Number of seconds it took to process the data used to create the Report Management File Set



NOTE

Report Management File Sets that are in the Recycle Bin display with a red background. (See "Restore Report Management File Sets from the Recycle Bin" on page 133 and "Empty Report Management File Sets from the Recycle Bin" on page 132 for more information.)

4. (Optional) In the **Max Items** box on the lower-right corner of the window, you can type the maximum number of Report Management File Sets to appear in the list, and then on the toolbar click **Refresh**.

See "Report Management Overview" on page 224 for access to information about the contents of Report Management File Sets and configuration options for Report Management Jobs. See the following related sections for tasks you can perform for the Report Management File Sets that are already in the system.

- See "Filter the Report Management File Sets List" on the facing page for instructions to complete this task.
- See "Refresh the Report Management File Sets List" on page 130 for instructions to complete this task.
- See "Print the Report Management File Sets List" on page 130 for instructions to complete this task.
- See "Roll Back Report Management File Sets" on page 131 for instructions to complete this task.
- See "Export Report Management File Sets" on page 132 for instructions to complete this task.
- See "Empty Report Management File Sets from the Recycle Bin" on page 132 for a list of data group types you can import.
- See "Restore Report Management File Sets from the Recycle Bin" on page 133 for instructions to complete this task.
- See "View Report Management File Sets Properties" on page 134 for instructions to complete this task.

Filter the Report Management File Sets List

To find specific Report Management File Sets more easily, you can apply filter criteria to the list of Report Management File Sets.

To filter the Report Management File Sets list

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Data Storage**.
3. On the right pane, click **Report Management File Sets**. Do one of the following:
 - Double-click the selected item.
 - On the **Action** menu, point to **All Tasks**, and then click **Report Management File Sets**.
 - On the toolbar, click **Report Management File Sets**.
 - Right-click the selected item, and then click **Report Management File Sets**.
4. Do one of the following:
 - On the **Action** menu, click **Filter**.
 - On the toolbar, click **Filter**.
5. In the **Data Storage Filter** dialog box, you can specify the following filter criteria:
 - In the **File Set Name** box, type the system-assigned name for the Report Management File Set.
 - In the **Finished** boxes, type the date range for when updates occurred to the Report Management File Set in the **YYYY-MM-DD hh:nn:ss** format. (See "Date and Time Format Information" on page 23 for more information.)
 - In the **Job Name** box, type the name of the Report Management Job that processed the Report Management File Set.
 - In the **Data Group** box, type the original data group name to which the Report Management File Set was appended.
 - In the **Imported** list, select the imported state of the Report Management File Set.
6. Click **OK**.



N O T E

Below the listed results, the number of items displayed appears followed by **(Filtered)** to indicate that a filter is applied to the Report Management File Sets list.

To remove a filter from the Report Management File Sets list

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Data Storage**.
3. On the right pane, click **Report Management File Sets**. Do one of the following:
 - Double-click the selected item.
 - On the **Action** menu, point to **All Tasks**, and then click **Report Management File Sets**.

- On the toolbar, click **Report Management File Sets**.
 - Right-click the selected item, and then click **Report Management File Sets**.
4. Do one of the following:
 - On the **Action** menu, click **Filter**.
 - On the toolbar, click **Filter**.
 5. In the **Data Storage Filter** dialog box, click **Clear Filter**, and then click **OK**.

Refresh the Report Management File Sets List

To ensure the Report Management File Sets list contains the most current information, you can manually refresh it.

To refresh the Report Management File Sets list

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Data Storage**.
3. On the right pane, click **Report Management File Sets**. Do one of the following:
 - Double-click the selected item.
 - On the **Action** menu, point to **All Tasks**, and then click **Report Management File Sets**.
 - On the toolbar, click **Report Management File Sets**.
 - Right-click the selected item, and then click **Report Management File Sets**.
4. Do one of the following:
 - On the **Action** menu, click **Refresh**.
 - On the toolbar, click **Refresh**.

Print the Report Management File Sets List

You can print the list of Report Management File Sets as it appears on the **Report Management File Sets** window.

To print the Report Management File Sets list

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Data Storage**.
3. On the right pane, click **Report Management File Sets**, and then do one of the following:
 - Double-click the selected item.
 - On the **Action** menu, point to **All Tasks**, and then click **Report Management File Sets**.
 - On the toolbar, click **Report Management File Sets**.
 - Right-click the selected item, and then click **Report Management File Sets**.
4. On the **Report Management File Sets** window, do one of the following:
 - On the **Action** menu, click **Print**.
 - On the toolbar, click **Print**.
5. In the **Print** dialog box, specify the print options, and then click **OK**.

Roll Back Report Management File Sets

Rolling back a Report Management File Set deletes data it contains. This function is useful to remove Report Management File Sets created by an incorrectly-configured Report Management Job without affecting the rest of the information in the data group. How the deletion of data is handled during the roll back process depends on the Read/Write state of the data group to which the Report Management File Set is appended and project Recycle Bin settings. Before rolling back Report Management File sets, review how the following items affect the roll back process.

- Project Recycle Bin settings determine whether Report Management File Sets are permanently deleted or placed in the Recycle Bin when they are rolled back. If the data groups to which the Report Management File Sets are appended contain multiple projects, the Recycle Bin settings for those projects must be the same, or you will not be able to roll back the Report Management File Sets. (See "Edit Project Properties" on page 162 for instructions to set Recycle Bin options.)
- If the data groups to which the Report Management File Sets are appended are in a **Read/Write** state, when you roll back the Report Management File Sets (and the project does not recycle documents), the actual data files are deleted from their storage location, along with the index values and reference pointers stored in the database. This information can not be restored. (See "Edit Data Group Properties" on page 118 to change the Read/Write state of a single data group and "Change the Read/Write State for All Data Groups" on page 114 to change the Read/Write state for all data groups.)
- If the data groups to which the Report Management File Sets are appended are in a **Read Only** state, when you roll back the Report Management File Sets (and the project does not recycle documents), only the index values and reference pointers stored in the database are deleted. No actual data files are deleted.



CAUTION

Use caution when rolling back Report Management File Sets that are appended to data groups in a Read/Write state, as you may permanently delete data.

To roll back Report Management File Sets

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Data Storage**.
3. On the right pane, click **Report Management File Sets**. Do one of the following:
 - Double-click the selected item.
 - On the **Action** menu, point to **All Tasks**, and then click **Report Management File Sets**.
 - On the toolbar, click **Report Management File Sets**.
 - Right-click the selected item, and then click **Report Management File Sets**.
4. On the **Report Management File Sets** window, select the Report Management File Set(s) to roll back (hold down the Ctrl key to select multiple items).
5. Do one of the following:
 - On the **Action** menu, point to **File Sets**, and then click **Roll Back**.
 - On the toolbar, click **Roll Back**.

- Right-click the selected item(s), and then click **Roll Back**.
6. Read the message that appears, and if you want to proceed, click **Yes** to confirm the roll back operation.

Export Report Management File Sets

You can export Report Management File Sets into an XML file.

To export Report Management File Sets

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Data Storage**.
3. On the right pane, click **Report Management File Sets**, and then do one of the following:
 - Double-click the selected item.
 - On the **Action** menu, point to **All Tasks**, and then click **Report Management File Sets**.
 - On the toolbar, click **Report Management File Sets**.
 - Right-click the selected item, and then click **Report Management File Sets**.
4. On the **Report Management File Sets** window, select the Report Management File Set(s) to export (hold down the Ctrl key to select multiple items).
5. Do one of the following:
 - On the **Action** menu, point to **File Sets**, and then click **Export**.
 - On the toolbar, click **Export**.
6. On the confirmation message, click **Yes**.
7. In the **Export File Set Entries** dialog box, select the location where the export file will go.
8. In the **File name** box, type a name for the export file, and then click **Save**.

Empty Report Management File Sets from the Recycle Bin

Whether Report Management File Sets appear in the Recycle Bin after they are rolled back depends on the Recycle Bin settings for the project. (See "Edit Project Properties" on page 162 for instructions to set Recycle Bin options.) Report Management File Sets that are in the Recycle Bin display with a red background. You can view the date and time it was recycled and by whom in the Report Management File Sets properties. (See "View Report Management File Sets Properties" on page 134 for instructions to open Report Management File Sets properties.)

The date and time is recorded when the Report Management File Set is initially rolled back, and it is not updated. For example, if you roll back a Report Management File Set, its properties show the date and time it was sent to the Recycle Bin. If you later select all Report Management Files Sets, and then roll them back, the original date and time of the previously rolled back Report Management File Set is not updated.

What happens to Report Management File Set data when you empty the Recycle Bin depends on the Read/Write state of the data group to which it is appended. Before emptying the Recycle Bin, review how the following items affect the data.

- If the data groups to which the Report Management File Sets are appended are in a **Read/Write** state, when you empty the Recycle Bin, the actual data files are deleted from their storage location, along with the index values and reference pointers stored in the database. This information

can not be restored. (See "Edit Data Group Properties" on page 118 to change the Read/Write state of a single data group and "Change the Read/Write State for All Data Groups" on page 114 to change the Read/Write state for all data groups.)

- If the data groups to which the Report Management File Sets are appended are in a **Read Only** state, when you empty the Recycle Bin, only the index values and reference pointers stored in the database are deleted. No actual data files are deleted.



C A U T I O N

Use caution when emptying Report Management File Sets that are appended to data groups in a Read/Write state from the Recycle Bin, as you may permanently delete data.

To empty Report Management File Sets from the Recycle Bin

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Data Storage**.
3. On the right pane, click **Report Management File Sets**. Do one of the following:
 - Double-click the selected item.
 - On the **Action** menu, point to **All Tasks**, and then click **Report Management File Sets**.
 - On the toolbar, click **Report Management File Sets**.
 - Right-click the selected item, and then click **Report Management File Sets**.
4. On the **Report Management File Sets** window, select the recycled Report Management File Set(s) to empty from the Recycle Bin (hold down the Ctrl key to select multiple items).
5. Do one of the following:
 - On the **Action** menu, point to **File Sets**, and then click **Empty from Recycle Bin**.
 - Right-click the selected item(s), and then click **Empty from Recycle Bin**.
6. Read the message that appears, and if you want to proceed, click **Yes** to confirm the empty operation.

Restore Report Management File Sets from the Recycle Bin

Whether Report Management File Sets appear in the Recycle Bin after they are rolled back depends on the Recycle Bin settings for the project. (See "Edit Project Properties" on page 162 for instructions to set Recycle Bin options.) Report Management File Sets that are in the Recycle Bin display with a red background. You can view the date and time it was recycled and by whom in the Report Management File Sets properties. (See "View Report Management File Sets Properties" on the next page for instructions to open Report Management File Sets properties.)

To restore Report Management File Sets from the Recycle Bin

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Data Storage**.
3. On the right pane, click **Report Management File Sets**. Do one of the following:
 - Double-click the selected item.
 - On the **Action** menu, point to **All Tasks**, and then click **Report Management File Sets**.

- On the toolbar, click **Report Management File Sets**.
 - Right-click the selected item, and then click **Report Management File Sets**.
4. On the **Report Management File Sets** window, select the recycled Report Management File Set(s) to restore from the Recycle Bin (hold down the Ctrl key to select multiple items).
 5. Do one of the following:
 - On the **Action** menu, point to **File Sets**, and then click **Restore from Recycle Bin**.
 - Right-click the selected item(s), and then click **Restore from Recycle Bin**.
 6. Click **Yes** to confirm the restore operation.

View Report Management File Sets Properties

The properties for Report Management File Sets display the following information:

- Start date and time for when the first updates occurred to the Report Management File Set
- Finish date and time for when the last updates occurred to the Report Management File Set
- Name of the Report Management Job that processed the Report Management File Set
- Workstation on which the automation service processed the data for the Report Management File Set
- Data group to which the Report Management File Set was appended
- Unique name for the Report Management File Set assigned by the system
- Number of documents contained in the Report Management File Set
- Number of pages contained in the Report Management File Set
- Size of the Report Management File Set in bytes
- Number of seconds it took to process the data used to create the Report Management File Set
- Files that were included in the Report Management File Set, and their source location
- For a recycled Report Management File Set, the date and time it was recycled and by whom appear in red text. The date and time stamp is recorded when the Report Management File Set is initially rolled back, and it is not updated. For example, if you roll back a Report Management File Set, its properties show the date and time it was sent to the Recycle Bin. If you later select all Report Management File Sets, and then roll them back, the date and time stamp of the previously rolled back Report Management File Set is not updated.

To view properties for Report Management File Sets

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Data Storage**.
3. On the right pane, click **Report Management File Sets**. Do one of the following:
 - Double-click the selected item.
 - On the **Action** menu, point to **All Tasks**, and then click **Report Management File Sets**.
 - On the toolbar, click **Report Management File Sets**.
 - Right-click the selected item, and then click **Report Management File Sets**.

4. On the **Report Management File Sets** window, select the Report Management File Set.
5. Do one of the following:
 - Double-click the selected item.
 - On the **Action** menu, point to **File Sets**, and then click **Properties**.
 - On the toolbar, click **Properties**.
 - Right-click the selected item, and then click **Properties**.
6. When you are finished viewing the properties, click **Close**.

General Security

A robust security architecture lets system administrators control nearly every aspect of system access. Under **General Security** you can:

- Configure and manage encryption keys
- Specify and manage system-wide security policies
- Specify and manage user rights for groups and individual users

To access general security options

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **General Security**.

For information about the items under **General Security**, see the following:

- See "Encryption Keys" below for instructions to configure and manage encryption keys.
- See "Security Policy" on page 137 for access to instructions to specify and manage system-wide security settings.
- See "System Groups" on page 142 for instructions to set up and manage rights for groups of users.
- See "System Users" on page 144 for instructions to set up and manage rights for individual users.

Encryption Keys

Encryption is an effective way to achieve data security, and the encryption of data at rest is supported. The encryption process uses an encryption key that turns data into an unreadable cipher through complex algorithms. An encryption key is a random string of bits created explicitly for encrypting and decrypting data. Encryption keys are designed with algorithms intended to ensure that every key is unpredictable and unique. The encryption process uses the following design:

- Algorithm: Rijndael – AES (256-bit)
- Encryption Mode: CBC (Cipher Block Chaining)
- Padding Method: FIPS81 (Federal Information Processing Standards 81) scheme (ISO10126)
- Secret Key Generation: User-defined pass phrase is passed through the SHA-2 algorithm (Secure Hashing Algorithm) to generate a 256-bit hash

After you add an encryption key, you can use it for numerous purposes. For example, you can specify an encryption key to encrypt data groups, report archives, and migration job data as it is stored (encryption of data at rest).

To add an encryption key

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **General Security**.
3. Click **Encryption Keys**.
4. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **New Encryption Key**.
 - On the toolbar, click **New**.
 - Right-click the selected item, and then click **New Encryption Key**.
5. In the **Key Name** box, type the name to identify the key.
6. In the **Key Type** list, select the type of encryption to use for this key.
7. In the **Pass Phrase** box, type the pass phrase for the key.
8. In the **Description** box, type a description for the encryption key.
9. Click **OK** to save the encryption key.

To refresh the encryption key list

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **General Security**.
3. Click **Encryption Keys**.
4. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Refresh**.
 - On the toolbar, click **Refresh**.
 - Right-click the selected item, and then click **Refresh**.

To delete encryption keys



C A U T I O N

Use caution when deleting encryption keys! Encrypted data becomes unreadable when the key used to encrypt the data is deleted.

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **General Security**.
3. Click **Encryption Keys**.
4. On the right pane, select the encryption key(s) to delete (hold down the Ctrl key to select multiple items).
5. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Delete**.
 - On the toolbar, click **Delete**.

- Right-click the selected item, and then click **Delete**.
6. Read the message that appears, and if you want to proceed, click **Yes** to confirm the deletion.

To edit encryption key properties



NOTE

After an encryption key is added, you can modify only its description. This prevents data that is encrypted with the key from becoming unreadable.

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **General Security**.
3. Click **Encryption Keys**.
4. On the right pane, select the encryption key.
5. Do one of the following:
 - Double-click the selected encryption key.
 - On the **Action** menu, point to **All Tasks**, and then click **Properties**.
 - On the toolbar, click **Properties**.
 - Right-click the selected item, and then click **Properties**.
6. In the **Encryption Key Properties** dialog box, modify the description, and then click **OK** to save the changes.

Security Policy

Under **Security Policy**, you can configure security policies. Security policies are set at the entity level, and let you define system-wide security settings.

To access security policies configuration

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **General Security**.
3. Click **Security Policy**.
4. Do one of the following:
 - On the right pane, double-click **Configure Security Policy**.
 - On the **Action** menu, point to **All Tasks**, and then click **Configure Security Policy**.
 - On the toolbar, click **Configure**.

For information about the properties on each tab of the **Entity Security Policy** dialog box, see the following:

- See "General Security Policy" on the next page for information about specifying properties on the **General** tab.
- See "Account Lockout Security Policy" on page 140 for information about specifying properties on the **Account Lockout** tab.
- See "Authentication Security Policy" on page 140 for information about specifying properties on the **Authentication** tab.

- See "Passwords Security Policy" on page 141 for information about specifying properties on the **Passwords** tab.

General Security Policy

The **General** security policy specifies general security options, user session settings, and encryption key and pass phrase assignments.

To set general security options

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **General Security**.
3. Click **Security Policy**, and then, on the right pane double-click **Configure Security Policy**.
4. In the **Entity Security Policy** dialog box, click the **General** tab.
5. You can set the following items:
 - **Require all session requests to originate from same source** - If selected, all session activity is required to originate from the source of the original log in. This ensures that user sessions cannot be taken over to gain unauthorized access to documents. When a user logs in, the IP address (or computer name) used to gain access is tracked, and each time information is requested, the system verifies that the request originated from that same IP address (or computer name). If not, the request for information is denied, and a notification is sent to the system administrators.
 - **Require web clients to use the browser plugin** - For version 84 and later, this option is deprecated and no longer functions.
 - **Enable Integrated Windows Authentication** - For version 84 and later, this option is deprecated and no longer functions.
 - **Disable encrypted document grant URLs** - If selected, document grant URLs are passed unencrypted, which makes the URLs considerably shorter. Although guessing a grant ID (which is a GUID) would be difficult, disabling the document grant URL encryption opens a potential vulnerability. You should weigh the benefits of a considerably shorter URL against the loss of security provided by encrypting the URL. If this option is selected, the application accepts both encrypted and unencrypted incoming (look up) grants. If this option is not selected, the system allows only the retrieval of encrypted grants.
 - **Graphically sign image-based documents** - If selected, all existing signatures stay with documents, unless the **Disable signature duplication when signing image-based documents** option (described below) is selected. If cleared, when documents are checked in, all existing signatures are removed, as they are no longer valid for the new version. This also applies to all non-imaged based documents.
 - **Disable signature duplication when signing image-based documents** - If selected, old signatures are not carried forward on each new version of image-based documents.
 - **Perform non-repudiation checks on documents** - If selected, non-repudiation checks are performed on all imported documents. The non-repudiation check absolutely ensures that the document was not tampered with. This option is selected by default.

To set the maximum session idle time

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **General Security**.

3. Click **Security Policy**, and then, on the right pane double-click **Configure Security Policy**.
4. Click the **General** tab.
5. In the **Session Cleanup** area, you can set the following item:
 - **Max. session idle time (minutes)** - This setting specifies the number of minutes that a user session can be idle before the session is automatically terminated and the user is logged out of the system. This value cannot exceed the value assigned in the General System Settings by the global administrator.

To assign encryption keys



NOTE

Before you can assign encryption keys, you must first add them. See "Encryption Keys" on page 135 for instructions.

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **General Security**.
3. Click **Security Policy**, and then, on the right pane double-click **Configure Security Policy**.
4. Click the **General** tab.
5. In the **Encryption Key Assignment** area, you can assign encryption keys to the following items:
 - **Cached Docs** - This setting specifies the encryption key used to encrypt cached documents. When a PaperVision Enterprise application server caches documents to be accessed by users, it temporarily places them at a location where the PaperVision Viewer can retrieve the document and then remove it. When you specify an encryption key, the application server uses it to encrypt the document being placed at the cache location. When the PaperVision Viewer retrieves the encrypted document, it decrypts it using the same key.



NOTE

Cached documents are encrypted only when the PaperVision Viewer is used, otherwise there is no mechanism to decrypt the documents.

- **Data Groups** - This setting specifies the encryption key used to encrypt data as it is stored (encryption of data at rest). See "Encrypt and Decrypt Data Groups" on page 110 for additional information.
- **Report Archives** - This setting specifies the encryption key used to encrypt report archives (encryption of data at rest). This setting is available only when hosting licensing is enabled and the PaperVision Enterprise installation has hosting capabilities.
- **Migration Jobs** - This setting specifies the encryption key used to encrypt migration job data as it is stored (encryption of data at rest). When migrating to zip files, the encryption key specified for migration jobs is used as the password for the zip files.

To set the pass phrase for inter-process communications

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **General Security**.

3. Click **Security Policy**, and then, on the right pane double-click **Configure Security Policy**.
4. Click the **General** tab.
5. In the **Inter-Process Communications** area, you can set the following item:
 - **Pass Phrase** - This setting specifies the pass phrase for the authentication of remote applications. For example, when automated external applications, such as the PaperVision Enterprise Message Capture Server connect to retrieve information, such as Message Capture Policies, this pass phrase is used to authenticate the connection.

Account Lockout Security Policy

The **Account Lockout** security policy determines whether user accounts get locked by the system, how many invalid login attempts can occur before a user account is locked, and whether the locked account and the lockout counters are automatically reset after a specified number of minutes. Even if the account lockout security policy is set to automatically unlock a locked account after a specified number of minutes, you can manually unlock the account before the specified time has elapsed. (See "Locked Users" on page 94 for instructions.)

To set the maximum session idle time

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **General Security**.
3. Click **Security Policy**, and then, on the right pane double-click **Configure Security Policy**.
4. In the **Entity Security Policy** dialog box, click the **Account Lockout** tab.
5. You can set the following items:
 - **Accounts never lockout** - If selected, user accounts are never locked out, regardless of the number of unsuccessful login attempts.
 - **Accounts lockout after X invalid attempts** - If selected, user accounts are locked out when the number of consecutive failed login attempts reaches the number you specify.
 - **Reset locked accounts after X minutes** - If selected, locked user accounts are automatically unlocked after the number of minutes you specify is reached.
 - **Clear lockout counters after X minutes** - If selected, lockout counters are reset if the user has not attempted to log in with an incorrect password during the number of minutes you specify. Every time a user attempts to log in with an incorrect password, a counter records the number of failed attempts since the last successful login. If this option is cleared, the counter is reset to zero only after the user successfully logs in.

Authentication Security Policy

The **Authentication** security policy specifies login restrictions and the encryption key assigned to the remote authentication gateway. See the following sections to learn more about remote authentication.

- See "Remote Authentication Functional Overview" on page 336 for a description of how remote authentication works.
- See "Remote Authentication Use Scenarios" on page 336 for likely remote authentication scenarios and their general installation steps.
- See "Configure PaperVision Authentication Gateway Settings" on page 338 for instructions to set up remote authentication.

To set login restrictions

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **General Security**.
3. Click **Security Policy**, and then, on the right pane double-click **Configure Security Policy**.
4. In the **Entity Security Policy** dialog box, click the **Authentication** tab.
5. In the **Login Restrictions** area, you can set the following items:
 - **Allow logins from any source** - If selected, users can log in from any IP address.
 - **Allow logins from only these IP addresses/subnets** - If selected, you must specify the IP addresses/subnets (described below) from which users are allowed to log in. Using this feature ensures that access can be gained only from specific locations.
 1. Click **Add**, and then in the **IP Address/Subnet** box, do one of the following:
 - To specify a particular address, type the exact address.
 - To specify a specific subnet, enter only the first **X** octets of the network (for example, typing 10.1 or 10.1.0.0 will specify the entire 10.1 class B address space).
 2. Click **OK**.

To assign an encryption key to the remote authentication gateway

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **General Security**.
3. Click **Security Policy**, and then, on the right pane double-click **Configure Security Policy**.
4. In the **Entity Security Policy** dialog box, click the **Authentication** tab.
5. In the **Remote Authentication Encryption Key Assignment** area, from the **Key Name** list, select the encryption key that has a value that matches the **Encryption Key Value** specified in the PaperVision Gateway Settings application located on the installed PaperVision Authentication Gateway Server.

Passwords Security Policy

The **Passwords** security policy lets you set parameters for password expiration, length, and complexity.

To set password options

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **General Security**.
3. Click **Security Policy**, and then, on the right pane double-click **Configure Security Policy**.
4. In the **Entity Security Policy** dialog box, click the **Passwords** tab.
5. You can set the following items:
 - **User passwords never expire** - If selected, user passwords never expire for the entity.
 - **User passwords expire in: X days** - If selected, user passwords automatically expire after the number of days you specify. When users with expired passwords attempt to log in, they must change their passwords.
 - **Expire All Passwords** - When you click this option, all user passwords are immediately expired so that all users must change their passwords when they attempt to log in.

- **No minimum password length** - If selected, user passwords can be any length, including blank.
- **Minimum password length: X characters** - If selected, when users reset their passwords, they must contain at least the number of characters you specify.
- **Password must contain upper case letters** - If selected, when users reset their passwords, they must contain at least one uppercase letter.
- **Password must contain lower case letters** - If selected, when users reset their passwords, they must contain at least one lowercase letter.
- **Password must contain numeric characters** - If selected, when users reset their passwords, they must contain at least one numeric character.
- **Password must contain special characters** - If selected, when users reset their passwords, they must contain at least one special character letters.
- **Allow password reset requests**- If selected, users can click a link when logging in to request an email message with instructions to reset their password. If users do not have **User can change password when desired** permission, then the email message will state that they do not have permission to change their password. (See "To add a system user" on page 144 for instructions to set the **User can change password when desired** permission.)

System Groups

After you have created user accounts, you can define groups of users who have similar access and functionality needs. (See "System Users" on page 144 for instructions to create user accounts.)

Creating system groups lets you assign access more efficiently, as you specify it only once for the group, rather than for each user. You can assign groups access to specific projects, and groups are used in defining WorkFlows. You can create, modify, and delete system groups.

To view system groups

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **General Security**.
3. Click **System Groups**.

The right pane shows a listing of defined user groups.

To add a system group



N O T E

Before you can create groups, user accounts must exist. See "System Users" on page 144 for instructions to create user accounts.

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **General Security**.
3. Click **System Groups**.
4. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **New Group**.
 - On the toolbar, click **New**.

- Right-click the selected item, and then click **New Group**.
5. In the **New Group** dialog box, in the **Group Name** box, type a name to identify the group of users.
 6. In the **Available Users** list, select the user(s) to include in the group (hold down the Ctrl key to select multiple users). (To include all available users, click **Select All** below the **Available Users** list.)
 7. Click the right arrow to move the selected users to the **Group Members** list.
 8. (Optional) To remove users from the group, in the **Group Members** list, select the user(s) to remove, and then click the left arrow. (To remove all users from the group, click **Select All** below the **Group Users** list, and then click the left arrow.)
 9. After you have defined the group, click **OK** to save it.

To refresh the system groups list

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **General Security**.
3. Click **System Groups**.
4. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Refresh**.
 - On the toolbar, click **Refresh**.
 - Right-click the selected item, and then click **Refresh**.

To delete system groups

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **General Security**.
3. Click **System Groups**.
4. On the right pane, select the system group(s) to delete (hold down the Ctrl key to select multiple items).
5. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Delete**.
 - On the toolbar, click **Delete**.
 - Right-click the selected item, and then click **Delete**.
6. Click **Yes** to confirm the deletion.

To edit system group properties



NOTE

After a group is created, you cannot modify its name. You can modify only its members. Modifications take effect the next time group members log in.

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **General Security**.

3. Click **System Groups**.
4. On the right pane, select the system group.
5. Do one of the following:
 - Double-click the selected item.
 - On the **Action** menu, point to **All Tasks**, and then click **Properties**.
 - On the toolbar, click **Properties**.
 - Right-click the selected item, and then click **Properties**.
6. To add users to the group, in the **Available Users** list, select the users to include in the group, and then click the right arrow. (To include all available users, click **Select All** below the **Available Users** list, and then click the right arrow.)
7. To remove users from the group, in the **Group Members** list, select the users to remove, and then click the left arrow. (To remove all users from the group, click **Select All** below the **Group Users** list, and then click the left arrow.)
8. When you are finished modifying the group, click **OK** to save the changes.

System Users

You must create a user account for each person who uses PaperVision Enterprise. You can create, import, modify, and delete system users. You can also assign and reset passwords for system users. You can create user accounts manually or you can use a pipe-delimited (or tab-delimited) text file to batch load user information. After you have created user accounts, you can define groups of users who have similar access and functionality needs. (See "System Groups" on page 142 for instructions to create user groups.) You can assign access to projects at the group and individual user level.

To view system users

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **General Security**.
3. Click **System Users**.

The right pane shows a listing of system users.

To add a system user

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **General Security**.
3. Click **System Users**.
4. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **New User**.
 - On the toolbar, click **New**.
 - Right-click the selected item, and then click **New User**.
5. In the **New User** dialog box, in the **User Name** box, type the name that will be used to log in.
6. (Optional) In the **Full Name** box, type the user's full name. (The user's full name is referenced in some reports.)

7. (Optional) In the **Email Address** box, type the user's email address that will receive system notifications (if configured to do so.)
8. In the **Password** box, type the initial password the user will use to log in.
9. In the **Confirm Password** box, type the user's password again to confirm it.

**NOTE**

We recommend that you never leave a password set to a blank value, as it can pose a security risk.

10. To force the user to change the password the next time they log in, select **User must change password at next login**.
11. To allow the user to change the password at any time, select **User can change password when desired**.
12. In the **Administration Rights** area, select the appropriate user type. To create a regular user, clear all of the check boxes. You can specify the following user types.
 - **System Administrator** - When you select this check box, the user can configure all administrative settings for the entity and has access to all functionality in all projects. However, system administrators cannot assign the entity's data group, full-text, migration, and batch paths; these path assignments require a global administrator.

**NOTE**

If you select **System Administrator**, the other user types are automatically assigned to the user.

- **Workflow Administrator** - When you select this check box, the user can design and configure workflows within the entity. They can configure workflow definitions for any project and view workflow history and workflow status reports, but they have no access to documents or functions in any projects unless a system administrator explicitly grants them access. If they have access to view documents within a project, workflow administrators can create workflow instances for a particular document and view its workflow status.
 - **Capture Administrator** - When you select this check box, the user can configure jobs in the PaperVision Capture product. This setting is not used in PaperVision Enterprise, and Capture administrators have no administrative capabilities in PaperVision Enterprise.
 - **E-Form Administrator** - When you select this check box, the user can create E-Forms in PaperVision Enterprise.
13. Click **OK** to save the user.

To import users



NOTE

Before performing this procedure, make sure that you have a properly-formatted text file that contains user information. See "File Format for Importing Users" on page 148 for more information.

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **General Security**.
3. Click **System Users**, and then do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Import User/Password List**.
 - Right-click the selected item, and then click **Import User/Password List**.
4. In the **Import User/Password File** dialog box, select the text file that contains the user information, and then click **Open**.
5. Click **OK** in the confirmation message.



NOTE

Existing users are not recreated during the import process.

To refresh the system users list

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **General Security**.
3. Click **System Users**.
4. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Refresh**.
 - On the toolbar, click **Refresh**.
 - Right-click the selected item, and then click **Refresh**.

To set a user password

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **General Security**.
3. Click **System Users**.
4. On the right pane, select the user, and then do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Set Password**.
 - On the toolbar, click **Set Password**.
 - Right-click the selected item, and then click **Set Password**.

5. In the **Set Password** dialog box, in the **New Password** box, type the new password for the user.

**N O T E**

We recommend that you never leave a password set to a blank value, as it can pose a security risk. Remember that passwords are case-sensitive.

6. In the **Confirm Password** box, type the user's password again to confirm it.
7. Click **OK** to save the password, and then click **OK** in the confirmation message.

To delete system users

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **General Security**.
3. Click **System Users**.
4. On the right pane, select the system user(s) to delete (hold down the Ctrl key to select multiple items).
5. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Delete**.
 - On the toolbar, click **Delete**.
 - Right-click the selected item, and then click **Delete**.
6. Click **Yes** to confirm the deletion.

To edit system user properties

**N O T E**

After a system user is created, you cannot modify the user name. You can modify all other system user properties.

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **General Security**.
3. Click **System Users**.
4. On the right pane, select the system user.
5. Do one of the following:
 - Double-click the selected item.
 - On the **Action** menu, point to **All Tasks**, and then click **Properties**.
 - On the toolbar, click **Properties**.
 - Right-click the selected item, and then click **Properties**.
6. In the **User Properties** dialog box, make your changes. (See "To add a system user" on page 144 for a description of the properties.)
7. When you are finished modifying the user properties, click **OK** to save the changes.

File Format for Importing Users

If you have many system users, rather than adding them one at a time, you can import a user list to populate most of their configuration data. (See "To import users" on page 146 for instructions.) The user list must be in a pipe-delimited (|) or tab-delimited text file. Each line of the text file can contain the following information in this order:

- User Name
- Password
- Full Name
- Email Address
- Administrator Options (values shown below)
 - 0 specifies no administrative rights
 - 1 specifies system administrator
 - 2 specifies WorkFlow administrator
 - 4 specifies Capture administrator
 - 8 specifies E-Forms administrator



N O T E

To specify multiple administrator rights, add their values. For example, a value of 10 specifies that the user is a WorkFlow and E-Forms administrator.

- User must change password at the next log in (if value is 1)
- User can change password when desired (if value is 1)

Only the first two values (user name and password) are required on each line of text. If values are not specified, the default value of zero (0) is used. The following lines are some sample text of an import file.

```
jdoe|password|John Doe|JohnDoe@data.com|0|1|1
bjones|password|Becky Jones|BeckyJones@data.com|6|1|1
```

Migration Jobs

The migration feature lets you save documents into a new XML data group. The original documents are not altered, nor are they removed from PaperVision Enterprise. Migration jobs are fully automated, and you can migrate:

- Documents placed on a list (See the "List Options" and the "Migration Jobs" sections in the *PaperVision Enterprise User Guide* for more information.)
- Data groups (See "Migrate Data Groups" on page 112 for more information.)
- Projects (See "Submit Projects for Migration" on page 161 for more information.)

When documents are migrated, the following basic steps are performed:

1. After an item is submitted for migration, it appears on the **Migration Jobs** pane. (See "Status and Tasks for Submitted Migration Jobs" on the next page for more information.)
2. The automated migration operation (**Migration Jobs**) locates the documents in their original data groups, and then copies them to a separate location, where they are formatted into an XML data group. This data group can then be saved to any supported media type by an administrator.
3. After a migration job is processed, the system sends an email message to the entity administrator if your system is configured to do so.
4. If an error occurs while copying the files during the migration process, the error is documented in a **Migration Errors.txt** file that includes detailed information (including the applicable index information) about any files that couldn't be located. Those files do not get added to the migrated data group.



NOTE

When documents or projects are deleted, any associated documents on migration lists are automatically removed. When an entity is deleted, any associated lists or migration jobs are automatically removed.

See "Migration Job Configuration Options" below and "Status and Tasks for Submitted Migration Jobs" on the next page for more information.

Migration Job Configuration Options

Configure the following options for migration jobs:

- For migration jobs to be processed, you must configure the **Migration Jobs** automated operation. (See "Configure Automation Service Scheduling" on page 61 for instructions.)
- To allow users to submit documents for migration, at the project level, you must select the **Tag for Migration** option. (See "Add Project Security Access" on page 188 for instructions.)
- To assign an encryption key to migration jobs, you must first create the encryption key, and then specify it in the security policy for the entity. (See "To add an encryption key" on page 136 and "To assign encryption keys" on page 139 for instructions.)

- In the entity properties, you can specify settings for the size and packaging format of data groups, and whether administrators are notified when a migration job completes or fails. (See "General Entity Properties" on page 74 for instructions.)

See "Migration Jobs" on the previous page and "Status and Tasks for Submitted Migration Jobs" below for more information.

Status and Tasks for Submitted Migration Jobs

After migration jobs are submitted, you can view their status and properties, cancel them (if they haven't started processing), and resubmit them (if they have completed). For project migrations, you can edit jobs (if they haven't started processing) or copy them (if they are running or have finished processing).

See "Migration Jobs" on the previous page and "Migration Job Configuration Options" on the previous page for more information.



NOTE

You can perform migration job tasks at the global level and the entity level. Performing tasks at the global level lets you work with migration jobs for all entities.

To view the status of migration jobs

1. After you have logged in to the Administration Console, do one of the following:
 - To work at the global level, on the left pane expand **Global Administration**.
 - To work at the entity level, on the left pane, expand **Entities**, and then expand the appropriate entity.
2. Click **Migration Jobs**.

The right pane shows for each migration job the:

- Entity ID (Only if accessed under Global Administration.)
- Date and time of submission
- Next scheduled run date and time
- User who submitted the migration job
- Name of the migration job (only project migration names are user specified)
- Date and time when the migration job started and finished
- Number of documents in the migration job
- Size of the migration job in megabytes
- Number of minutes it took to complete the migration job

The following background colors indicate the status of each migration job:

- A white background indicates that the job has not been processed.
- An aqua background indicates that the job is currently running.
- A green background indicates that the job processed successfully.
- A red background indicates that an error occurred during the processing of the job.

- A yellow background indicates that the job was canceled.
- When you select a job, it appears with a blue background.

To refresh the list of migration jobs

1. After you have logged in to the Administration Console, do one of the following:
 - To work at the global level, on the left pane expand **Global Administration**.
 - To work at the entity level, on the left pane, expand **Entities**, and then expand the appropriate entity.
2. Click **Migration Jobs**.
3. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Refresh**.
 - On the toolbar, click **Refresh**.
 - Right-click the selected item, and then click **Refresh**.

To cancel a migration job

1. After you have logged in to the Administration Console, do one of the following:
 - To work at the global level, on the left pane expand **Global Administration**.
 - To work at the entity level, on the left pane, expand **Entities**, and then expand the appropriate entity.
2. Click **Migration Jobs**.
3. On the right pane, select the migration job, and then do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Cancel**.
 - On the toolbar, click **Cancel**.
 - Right-click the selected item, and then click **Cancel**.

To view properties for a migration job

1. After you have logged in to the Administration Console, do one of the following:
 - To work at the global level, on the left pane expand **Global Administration**.
 - To work at the entity level, on the left pane, expand **Entities**, and then expand the appropriate entity.
2. Click **Migration Jobs**.
3. On the right pane, select the migration job, and then do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Properties**.
 - On the toolbar, click **Properties**.
 - Right-click the selected item, and then click **Properties**.
 - Double-click the selected item.

The **Migration Job Properties** dialog box appears, and displays the:

- Name of the migration job (only project migration names are user specified)
- Migration ID (a system-generated unique identifier for the migration job)
- Entity name

- User who submitted the migration job
- Date and time when the migration job was submitted
- Next scheduled run date and time
- Date and time when the migration job started and finished
- Number of documents in the migration job
- Size of the migration job
- Amount of time it took to complete the migration job
- Message describing the status of the migration job
- **Data Groups, Lists, or Projects** tab. The tab that appears is based on the content of the migration job and displays the following information:
 - The **Data Groups** tab shows the data group name and the project ID for each data group included in the migration job.
 - The **Lists** tab shows the name of the list and the number of documents and projects included in the list.
 - The **Projects** tab shows the name of the project, the next document ID, and the next object ID.

To resubmit a user list or data group migration job

1. After you have logged in to the Administration Console, do one of the following:
 - To work at the global level, on the left pane expand **Global Administration**.
 - To work at the entity level, on the left pane, expand **Entities**, and then expand the appropriate entity.
2. Click **Migration Jobs**.
3. On the right pane, select the migration job, and then do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Properties**.
 - On the toolbar, click **Properties**.
 - Right-click the selected item, and then click **Properties**.
 - Double-click the selected item.
4. On the **Migration Job Properties** dialog box, click **Resubmit**.
5. On the confirmation messages, click **Yes**, and then click **OK**.

To copy a project migration job

1. After you have logged in to the Administration Console, do one of the following:
 - To work at the global level, on the left pane expand **Global Administration**.
 - To work at the entity level, on the left pane, expand **Entities**, and then expand the appropriate entity.
2. Click **Migration Jobs**.

3. On the right pane, select the project migration job, and then do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Properties**.
 - On the toolbar, click **Properties**.
 - Right-click the selected item, and then click **Properties**.
 - Double-click the selected item.
4. On the **Migration Job Properties** dialog box, click **Copy Job**.
5. In the **Project Migration** dialog box, set the options, and then click **OK**. (See "Submit Projects for Migration" on page 161 for information about project migration options.)
6. On the confirmation message, click **OK**.

To edit a project migration job



N O T E

You can edit a project migration job, only if the job has not started processing.

1. After you have logged in to the Administration Console, do one of the following:
 - To work at the global level, on the left pane expand **Global Administration**.
 - To work at the entity level, on the left pane, expand **Entities**, and then expand the appropriate entity.
2. Click **Migration Jobs**.
3. On the right pane, select the project migration job, and then do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Properties**.
 - On the toolbar, click **Properties**.
 - Right-click the selected item, and then click **Properties**.
 - Double-click the selected item.
4. In the **Migration Job Properties** dialog box, click **Edit Job**.
5. In the **Project Migration** dialog box, set the options, and then click **OK**. (See "Submit Projects for Migration" on page 161 for information about project migration options.)
6. On the confirmation message, click **OK**.

This page was intentionally inserted without content.



CHAPTER 5

Project Configuration

Project Configuration Overview	156
Add Projects	157
Refresh the Projects List	158
Delete Projects	158
Empty the Recycle Bin	158
Submit Projects for Full-Text Rebuild	159
Submit Projects for Full-Text Recreation	159
Submit Projects for Full-Text Compression	160
Submit Projects for Version Cleanup	160
Submit Projects for Migration	161
Edit Project Properties	162
Configure Index Fields	163



Project Configuration Overview

A project is a logical grouping of documents based on a common indexing schema. For example, ABC Company has three projects: Human Resources, Accounts Receivable, and Sales.

- The Human Resources project contains employee records and health insurance information.
- The Accounts Receivable project contains billing, purchase order, and invoice information.
- The Sales project contains prospect and client information.

Each of these projects is a separate logical grouping within the ABC Company entity. You can create projects manually, or they are automatically created when a data group is imported and the project referenced in the data group does not exist. Project names must be unique within an entity, but an administrator can create an unlimited number of projects. Projects support up to 200 named index fields per document.



IMPORTANT

Microsoft SQL Server supports maximum row sizes of 8060 characters. If the length of the combined index field data for a document exceeds 8060 characters, SQL Server cannot support it, and the system displays an alert.

To access project configuration functions

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Projects**.

The right pane shows a list of existing projects and shows for each project the:

- Identification Number
- Name

As you work with projects, see the following related sections for additional information.

- See "Add Projects" on the facing page for instructions to complete this task.
- See "Refresh the Projects List" on page 158 for instructions to complete this task.
- See "Delete Projects" on page 158 for instructions to complete this task.
- See "Empty the Recycle Bin" on page 158 for instructions to complete this task.
- See "Submit Projects for Full-Text Rebuild" on page 159 for instructions to complete this task.
- See "Submit Projects for Full-Text Compression" on page 160 for instructions to complete this task.
- See "Submit Projects for Migration" on page 161 for instructions to complete this task.
- See "Edit Project Properties" on page 162 for instructions to complete this task.
- See "Configure Index Fields" on page 163 for instructions to complete this task.

Add Projects

Projects are automatically added when a data group is imported and the project referenced in the data group does not exist, but you can also add projects manually. An administrator can create an unlimited number of projects, but project names must be unique within an entity. Projects support up to 200 named index fields per document.



IMPORTANT

Microsoft SQL Server supports maximum row sizes of 8060 characters. If the length of the combined index field data for a document exceeds 8060 characters, SQL Server cannot support it, and the system displays an alert.

When you add a project, the system automatically assigns it a project ID number. The numbering system starts at one and automatically increments each time you add a project. If you delete a project, its ID number is never reused.

To add a project

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Projects**.
3. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **New Project**.
 - On the toolbar, click **New**.
 - Right-click the selected item, and then click **New Project**.
4. In the **Project Name** box, type a unique name for the project.
5. In the **Max Revisions** box, type the maximum number of document revisions to retain when a document is checked back in. The oldest versions are automatically deleted or moved to the Recycle Bin based on the Recycle Bin settings for the project. If this value is set to zero, all revisions are kept.
6. In the **Recycle Bin Usage** area, you can set the following options that are selected by default:
 - **Document Deletion** - When selected, any document that is deleted from the project is moved to the Recycle Bin.
 - **Data Group/File Set Purging** - When selected, any data group, Message Capture File Set, or Report Management File Set that is purged from the project is moved to the Recycle Bin.
 - **Document Destruction Processing** - When selected, any document set to be destroyed in a Records Retention Policy Set, is moved to the Recycle Bin when the Records Retention Automation Service runs.
7. In the **Automatically Empty Recycle Bin** area, you can set one of the following options:
 - **Never** - When selected, the Recycle Bin is never emptied automatically. This is the default setting.
 - **After Being Recycled** - When selected, you specify the number of minutes, hours, or days after which a recycled item is automatically emptied from the Recycle Bin.
8. Go to step four in the "To add document index fields" on page 163 procedure for instructions to set up index fields for the project.

Refresh the Projects List

To ensure the projects list contains the most current information, you can manually refresh it.

To refresh the projects list

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Projects**.
3. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Refresh**.
 - On the toolbar, click **Refresh**.

Delete Projects

Deleting projects removes all of the project-related data from the system, but leaves the security audit data intact for reporting purposes. Deleting projects does not erase document files from their respective data groups. To erase document files, you must purge the data group.

To delete projects

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Projects**.
3. On the right pane, select the project to delete (hold down the Ctrl key to select multiple items).
4. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Delete**.
 - On the toolbar, click **Delete**.
 - Right-click the selected item, and then click **Delete**.
5. Click **Yes** to confirm the deletion.

Empty the Recycle Bin

What is in the Recycle Bin is determined by the **Recycle Bin Usage** settings for the project. (See "Edit Project Properties" on page 162 for a description of the Recycle Bin usage options.) When you empty the Recycle Bin, it creates a job on the Maintenance Queue to permanently delete the documents.

To empty the Recycle Bin

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Projects**.
3. On the right pane, select the project (hold down the Ctrl key to select multiple items).
4. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Empty Recycle Bin**.
 - On the toolbar, click **Empty Recycle Bin**.
 - Right-click the selected item, and then click **Empty Recycle Bin**.

5. In the **Empty Recycle Bin** dialog box, type the date and time on which or prior to documents must have been recycled for them to be deleted, and then click **OK**.
6. Click **Yes** to confirm the operation, and then click **OK** to close the confirmation message.

Submit Projects for Full-Text Rebuild

You can submit a project to have its full-text database rebuilt. This feature is useful if the full-text database has become corrupt or you want to change whether external and COLD documents are to be full-text indexed. When you submit a project for a full-text rebuild, it creates a job on the Maintenance Queue to be run by the automation service. When the job is run, each document is updated in the existing database, and documents remain available during the rebuild. Depending on the size and fragmentation level of the full-text database, it might be faster to use the full-text recreation option instead of the full-text rebuild. (See "Submit Projects for Full-Text Recreation" below for more information.)

To submit projects for full-text rebuild

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Projects**.
3. On the right pane, select the project to submit to rebuild the full-text indexes (hold down the Ctrl key to select multiple items).
4. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Submit for Full-Text Rebuild**.
 - On the toolbar, click **Submit for Full-Text Rebuild**.
 - Right-click the selected item, and then click **Submit for Full-Text Rebuild**.
5. Click **Yes** to confirm the operation, and then click **OK** to close the confirmation message.

Submit Projects for Full-Text Recreation

You can submit a project to have its full-text database recreated. This feature is useful if the full-text database has become corrupt or you want to change whether external and COLD document are to be full-text indexed. When you submit a project for a full-text recreation, it creates a job on the Maintenance Queue to be run by the automation service. When the job is run, the full-text database is deleted and each document is added again. Documents become searchable as they are added. If documents must remain available, then consider doing a full-text rebuild which leaves the database in place and updates each of the existing documents. (See "Submit Projects for Full-Text Rebuild" above for instructions.) Depending on the size and fragmentation level of the full-text database, it might be faster to use the full-text recreation option instead of the full-text rebuild.

To submit projects for full-text recreation

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Projects**.
3. On the right pane, select the project to submit to recreate the full-text indexes (hold down the Ctrl key to select multiple items).

4. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Submit for Full-Text Recreation**.
 - On the toolbar, click **Submit for Full-Text Recreation**.
 - Right-click the selected item, and then click **Submit for Full-Text Recreation**.
5. Click **Yes** to confirm the operation, and then click **OK** to close the confirmation message.

Submit Projects for Full-Text Compression

You can submit a project to have its full-text database compressed. This is useful if large amounts of information were deleted from the full-text database, such as when data groups are purged. When data is deleted from the full-text database, it is removed, but the space within the database is not reclaimed until a full-text compression is performed.

To submit projects for full-text compression

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Projects**.
3. On the right pane, select the project to submit for full-text compression (hold down the Ctrl key to select multiple items).
4. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Submit for Full-Text Compression**.
 - On the toolbar, click **Submit for Full-Text Compression**.
 - Right-click the selected item, and then click **Submit for Full-Text Compression**.
5. Click **Yes** to confirm the operation, and then click **OK** to close the confirmation message.

Submit Projects for Version Cleanup

You can submit a project for version cleanup. When you submit a project for version cleanup, it creates a job on the Maintenance Queue to be run by the automation service. When the job is run, each document in the project is evaluated against the maximum number of document revisions allowed according to the **Max Revisions** property. The oldest document versions are automatically deleted or moved to the Recycle Bin based on the Recycle Bin settings for the project. The maximum number of document revisions allowed and Recycle Bin settings are specified in the project properties. (See "Edit Project Properties" on page 162 for instructions.)

To submit projects for version cleanup

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Projects**.
3. On the right pane, select the project to submit for version cleanup (hold down the Ctrl key to select multiple items).
4. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Submit for Version Cleanup**.
 - On the toolbar, click **Submit for Version Cleanup**.
 - Right-click the selected item, and then click **Submit for Version Cleanup**.

5. Click **Yes** to confirm the operation, and then click **OK** to close the confirmation message.

Submit Projects for Migration

The migration feature lets you save documents into a new XML data group. The original documents are not altered, nor are they removed from PaperVision Enterprise. Migration jobs are fully automated, and for project-level migration jobs you can:

- Include one or more projects per migration job
- Run the project migration job once, or set up a recurring schedule
- Include new documents only, or new documents and versions
- Include or exclude document annotations

This section describes how to submit projects for migration. See the following sections for additional information.

- See "Migration Jobs" on page 149 for an overview of how migration jobs work.
- See "Migration Job Configuration Options" on page 149 for a description of these options and where to set them.
- See "Status and Tasks for Submitted Migration Jobs" on page 150 for instructions to work with submitted migration jobs.

To submit projects for migration

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Projects**.
3. On the right pane, select the project to submit for migration (hold down the Ctrl key to select multiple items).
4. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Submit for Migration**.
 - On the toolbar, click **Submit for Migration**.
 - Right-click the selected item, and then click **Submit for Migration**.
5. In the **Name** box, type a name for the migration job.
6. In the **Projects** area, you can do the following tasks:
 - To change the **Next Doc** value, select the project, and then click **Edit**. In the **Next Doc ID** box, type the value, and then click **OK**.



T I P

The **Next Doc** value keeps track of the starting document ID so that recurring migration jobs will include only documents that are new. You can modify this value to re-migrate or skip documents, or set this value to zero so that every document is migrated.

- To remove a project from the migration job, select it, and then click **Remove**.

7. In the **Documents to Migrate** area, select one of the following options:
 - **New Documents** – When selected, any new documents are included in the migration job.
 - **New Documents and Versions** – When selected, any new documents and the latest version of revised documents are included in the migration job.
8. To include document annotations, select **Include Annotations**.
9. Click the **Schedule** tab.
10. In the **Next Start Time** box, type the date for the next project migration. You can specify a time; otherwise, the default start time is midnight.
11. In the **Schedule List**, select either **<No Schedule - Run Once>** or select the unit of measure for the repetition.
12. If you selected a repetition schedule, in the **Repetition Schedule** area, specify the frequency of the schedule.
13. After you are done setting options for the project migration, click **OK**.
14. On the confirmation message, click **OK**.

The project migration job now appears on the **Migration Jobs** pane. (See "Status and Tasks for Submitted Migration Jobs" on page 150 for instructions to work with submitted migration jobs.)

Edit Project Properties

You can change project index fields and recycle bin settings at any time (even after the project contains documents). After an index field is created, it is added to all of the documents in the project. If there are existing documents that did not previously contain the index field, it is added to them with a blank value. When an index field is removed, all of the existing index field data for that field is deleted. When you add or remove an index field, the changes take place immediately.

To edit project properties

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Projects**.
3. On the right pane, select the project to edit.
4. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Properties**.
 - On the toolbar, click **Properties**.
 - Right-click the selected item, and then click **Properties**.
5. In the **Project Name Properties** dialog box, you can edit the following properties:
 - **Project Name** - Specifies a unique name for the project.
 - **Max Revisions** - Specifies the maximum number of document revisions to retain when a document is checked back in. The oldest versions are automatically deleted or moved to the Recycle Bin based on the Recycle Bin settings for the project. If this value is set to zero, all revisions are kept.
 - **Document Index Fields** - Specifies the index fields for the project. See "Configure Index Fields" on the facing page for instructions to work with index fields.

- **Recycle Bin Usage** - In this area, you can set the following options that are selected by default:
 - **Document Deletion** - When selected, any document that is deleted from the project is moved to the Recycle Bin.
 - **Data Group/File Set Purging** - When selected, any data group, Message Capture File Set, or Report Management File Set that is purged from the project is moved to the Recycle Bin.
 - **Document Destruction Processing** - When selected, any document set to be destroyed in a Records Retention Policy Set, is moved to the Recycle Bin when the Records Retention Automation Service runs.
- **Automatically Empty Recycle Bin** - In this area, you can set one of the following options:
 - **Never** - When selected, the Recycle Bin is never emptied automatically. This is the default setting.
 - **After Being Recycled** - When selected, you specify the number of minutes, hours, or days after which a recycled item is automatically emptied from the Recycle Bin.

6. After you are finished making changes, click **OK** to save the project.

Configure Index Fields

Document index fields are usually populated during the document capture process and contain essential data that identifies documents. You can then use these index field values to search for and retrieve documents in PaperVision Enterprise. Each document can contain up to 200 named index fields. You can create these index fields in the product you use to capture documents or when you set up the PaperVision Enterprise project.



IMPORTANT

Microsoft SQL Server supports maximum row sizes of 8060 characters. If the length of the combined index field data for a document exceeds 8060 characters, SQL Server cannot support it, and the system displays an alert.

When index field values are saved in PaperVision Enterprise, the following characters are automatically removed from them: % ^ & * | <

After an index field is created, it is added to all of the documents in the project. If there are existing documents that did not previously contain the index field, it is added to them with a blank value. When an index field is removed, all of the existing index field data for that field is deleted. When you add or remove an index field, the changes take place immediately.

To add document index fields

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Projects**.
3. On the right pane, select the project, and then do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Properties**.
 - On the toolbar, click **Properties**.
 - Right-click the selected item, and then click **Properties**.

4. In the **Document Index Fields** area, click **Add** to open the **Insert New Field** dialog box.
5. In the **Field Name** box, type the name of the new index field.



IMPORTANT

The following index field names are reserved for use by the Document Search Service. When creating index and detail field indexes, do not use the following values in the **Field Name** box. Doing so causes inaccurate search results in PaperVision Enterprise or ImageSilo. You can use variations of the names as long as they are not an exact match. For example, you cannot use the value **DOCID**, but **DOC_ID** and **DOCID1** are valid.

DOCCKEOUTTIME	DOCCKEOUTUSERID	DOCCKEOUTUSERNAME
DOCCREATEDATE	DOCDGID	DOCDGNAME
DOCDGORIGNAME	DOCFOLDERID	DOCFOLDERNAME
DOCFTINDEX	DOCDUPEID	DOCID
DOCRECRETDESTDATE	DOCRECRETDESTINFO	DOCRECRETLOCKDATE
DOCRECRETDESTLISTID	DOCRECRETLOCKINFO	DOCSECURELIST
DOCSIGDATETIME	DOCSIGID	DOCSIGNAME
DOCSIGUSERID	DOCSIGUSERFULLNAME	DOCSIGUSERNAME
DOCSOURCEDOCID	DOCSIGSOURCEIP	DOCWFDEFID
DOCWFENDTIME	DOCWFINSTID	DOCWFNAME
DOCWFSTARTTIME	OBJHASHTYPE	OBJID
OBJPAGES	OBJTRASHDATETIME	OBJTRASHUSERID
OBJTRASHUSERNAME	OBJTYPE	OBJVERSIONCREATOR
OBJVERSIONNUM	OBJVERSIONTIME	

6. In the **Field Type** list, select one of the following field types:
 - **Boolean** - This field type stores Boolean values such as Yes/No, On/Off, and True/False.
 - **Currency** - This field type stores currency (monetary) values.
 - **Date** - This field type stores date/time values between January 1, 1753 and December 31, 9999. This field type supports searches on date ranges.
 - **Double Number** - This field type stores numbers too large for a number field type or numbers that require decimal places. Numbers with more than 15 digits might display in scientific notation. This field type supports searches on number ranges.
 - **Long Text** - This field type stores text that exceeds 255 characters in length, and can store up to approximately 64,000 total characters. The content of long text fields is not indexed by the database server, so search time can be increased significantly when there are a large number of records.
 - **Number** - This field type stores whole-number values between -2,147,483,648 and 2,147,483,647. This field type supports searches on number ranges and hyphens or dashes at the beginning of the number to indicate a negative value. However, it does not support hyphens or dashes within the number, such as dashes within a social security number (555-55-5555). Exclude these dashes from the number.

- **Text** - This field type stores up to 255 characters of text.
- **Text(900)** - This field type stores up to 900 characters of text.

**I M P O R T A N T**

When documents that contain the Text(900) field type are migrated, the field content is truncated to 255 characters because the migration databases do not support this field type.

7. If you selected **Boolean**, **Currency**, **Date**, or **Double Number** for the field type, do one of the following:
 - In the **Field Format** list, select the format for the field contents.
 - Create a custom field format by typing directly in the **Field Format** box.
 For a **Boolean** field type, you must include a forward slash (/) between the two options. For example, Open/Closed or Single/Multiple. For a **Currency** field type, valid currency symbols include the dollar (\$), pound (£), euro (€), comma (,), and period (.).
8. In the **Automatically Add Wildcards** area, you can select one of the following options:
 - **None** - When selected, no wildcard characters are automatically added to search criteria for the index field. Users must manually type any wildcard characters in the search criteria.
 - **Start of Criteria** - When selected, wildcard characters are automatically added to the beginning of search criteria for the index field.
 - **End of Criteria** - When selected, wildcard characters are automatically added to the end of search criteria for the index field.
 - **Start and End of Criteria** - When selected, wildcard characters are automatically added to the beginning and the end of search criteria for the index field.
9. In the **Index Field Value List** area, you can specify options for field values that are used during searching, manually adding new documents, and editing index fields. Select one of the following options:
 - **Users Enter Ad Hoc Index Field Values** - When selected, users can enter any field value that the field type allows.
 - **Users Must Select Index Field Values From List** - When selected, users must select a field value from a predefined list of possible values.
 - **Users Enter Ad Hoc Index Field Values or Select From List** - When selected, users can enter any field value that the field type allows or select a field value from a predefined list of possible values.

10. To define a list of values for the index field, do the following:
 1. Click **Add** to open the **Add New Index Field Value** dialog box.
 2. In the box, type the index value(s) to appear in the list for the index field. Use a tilde (~) to separate each value (for example, value1~value2~value3).



NOTE

The number of pre-defined index values that will appear for users is limited to the first 1000 values. To see values beyond the first 1000, the user must type in the index box which causes the values to be filtered as they type.

3. Click **OK** to save the index values.
 4. To remove an index value from the list, select it, and then click **Remove**.
 5. To have the index values populated from the list provided in a PaperFlow data group, select the **Get Index Value List from Data Group** check box.
11. To have the system verify that index field information exists as a data group is imported or documents are uploaded or scanned, select the **Required** check box.

If you select the **Required** check box, when uploading or scanning documents, the operation will stop when a required index field is blank and the user receives a notification message.

When importing data groups, selecting the **Required** check box causes the import to skip any documents that have a blank required index field. If the **Required** check box and the **Halt import if missing required index fields** option are both selected, the import will immediately stop when a document that has a blank required index field is found. This feature is useful to identify data being imported that was not fully indexed. (See "To set import error handling" on page 81 for instructions to set the **Halt import if missing required index fields** option.)



NOTE

This option is not applicable to PaperVision Enterprise Report Management (ERMGROUP.XML) or PaperVision Message Capture (MSGGROUP.XML) data groups, as the file sets within them cannot be partially imported.

This option is automatically enabled when a PaperFlow data group is imported into a new project that was not created in PaperVision Enterprise, and the Required option in PaperFlow is selected.

12. To have the index field initiate a Workflow instance for a document, select the **Workflow Trigger** check box. (See "To add a pre-condition to a workflow definition" on page 269 for more information.)
 13. Click **OK** to save the new index field.
 14. Repeat steps 4 through 13 to add other index fields.
 15. After you are finished adding index fields, click **OK** to save the project properties.

To edit document index fields

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Projects**.
3. On the right pane, select the project, and then do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Properties**.
 - On the toolbar, click **Properties**.
 - Right-click the selected item, and then click **Properties**.
4. In the **Document Index Fields** area, select the document index field to edit.
5. Click **Edit** to open the **Edit Field** dialog box.
6. Modify the index field properties, and then click **OK**. (See the "To add document index fields" on page 163 procedure for a description of each property.)

To delete document index fields



CAUTION

Removing index fields from an existing project will permanently delete any data stored in those index fields.

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Projects**.
3. On the right pane, select the project, and then do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Properties**.
 - On the toolbar, click **Properties**.
 - Right-click the selected item, and then click **Properties**.
4. In the **Document Index Fields** area, select the document index field to delete (hold down the Ctrl key to select multiple items).
5. Click **Remove**, and then click **Yes** to confirm the deletion.

To add Message Capture index fields



TIP

If your site uses the PaperVision Message Manager product to process email messages for storage, you can add predefined Message Capture Index fields to the project. After the index fields are added, you can remove any unwanted ones and manually add others.

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Projects**.
3. On the right pane, select the project, and then do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Properties**.
 - On the toolbar, click **Properties**.
 - Right-click the selected item, and then click **Properties**.

4. In the **Document Index Fields** area, click the **Add Message Capture Fields** button (displays an envelope).
5. Click **Yes** to confirm the operation.

To reorder document index fields

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Projects**.
3. On the right pane, select the project, and then do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Properties**.
 - On the toolbar, click **Properties**.
 - Right-click the selected item, and then click **Properties**.
4. In the **Document Index Fields** area, select the document index field to move.
5. Click the up or down arrow button to move the document index field.
6. Click **OK** to save your changes.

CHAPTER 6

Project Administration

Enhanced Auditing	170
Document Associations	172
Document Security Levels	177
Integration Definitions	182
Security Access	188
Directory Manager Jobs	193
Records Destruction Lists	198
Records Retention Policy Sets	200



Enhanced Auditing

By default, every user operation is tracked so administrators can perform security audits and run utilization reports. (See "Report Functions" on page 296 for more information about reports.) You can also set up enhanced auditing for each project to provide detailed document tracking that can help you fulfill regulatory compliance obligations. When you enable enhanced auditing, each time users perform a document operation that could result in disclosure to another party, they are required to specify the following information:

- **Method of Disclosure** - Records how the information was disclosed, for example, via print, fax machine, email, and so on.
- **Disclosure Recipient** - Records who is receiving the information.
- **Disclosure Reason** - Records the reason the information was disclosed to the recipient.

Users can also add notes to provide additional information about the disclosure.

To configure enhanced auditing for a project

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Projects**.
3. Expand the appropriate project, click **Enhanced Auditing**, and then do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Configure General Settings**.
 - On the toolbar, click **Configure General Settings**.
 - Right-click the selected item, and then click **Configure General Settings**
 - On the right pane, double-click **General Settings**.
4. In the **Enhanced Auditing** dialog box, select **Enable Enhanced Auditing**.
5. In the **Disclosure Recipients** area, select one of the following options:
 - **Users must select Disclosure Recipients from list** - When selected, users must select a disclosure recipient from a predefined list.
 - **Users can enter ad hoc Disclosure Recipients** - When selected, users can enter any disclosure recipient or select a recipient from a predefined list.
 - **Add ad hoc Disclosure Recipients to list** - When selected, as new disclosure recipients are entered, they are added to the global list for others to select.
6. In the **Viewing Disclosure Reason** box, you can type a default reason why documents are viewed.

Because enhanced auditing requires that any disclosure (including viewing the document) is tracked, this value is recorded as the reason so that users do not have to manually specify a reason every time they open a document. However, users can override this value by manually specifying a viewing disclosure reason.
7. In the **Disclosure Reasons** area, select one of the following options:
 - **Users must select Disclosure Reasons from list** - When selected, users must select a disclosure reason from a predefined list.

- **Users can enter ad hoc Disclosure Reasons** - When selected, users can enter any disclosure reason or select a reason from a predefined list.
 - **Add ad hoc Disclosure Reasons to list** - When selected, as new disclosure reasons are entered, they are added to the global list for others to select.
8. Click **OK** to save the settings.
 9. See "Disclosure Reason List" below and "Disclosure Recipient List" on the next page for instructions to create these lists.

Disclosure Reason List

If you have set up enhanced auditing for a project, each time users perform a document operation that could result in disclosure to another party, they are required to specify who received the information and a reason for the disclosure of the information. (See "Disclosure Recipient List" on the next page for instructions to configure disclosure recipients.) You can configure your system to let users manually enter disclosure reasons or select them from a list of predefined values. You can also copy disclosure reasons from one project to another. This section describes how to configure disclosure reason lists. After a disclosure reason list is created, users can select values from it. If your enhanced auditing configuration allows it, as users manually enter disclosure reasons, they can be added to the list so others can use them. (See "Enhanced Auditing" on the previous page for instructions to configure enhanced auditing options.)

To configure disclosure reasons

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Projects**.
3. Expand the appropriate project, click **Enhanced Auditing**, and then do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Configure Disclosure Reason Lists**.
 - On the toolbar, click **Configure Disclosure Reason List**.
 - Right-click the selected item, and then click **Configure Disclosure Reason Lists**
 - On the right pane, double-click **Configure Disclosure Reason List**.
4. In the **Disclosure Reason List** dialog box, click **Add**.
5. In the box, type the disclosure reason(s) to appear in the list. Use a comma (,) to separate each reason (for example, reason1, reason2, reason3).
6. Click **OK** to save the disclosure reasons.
7. To remove a disclosure reason from the list, select it, click **Remove**, and then click **Yes** to confirm the operation.
8. To copy disclosure reasons from another project, complete the following steps:
 1. Click **Copy**.
 2. From the list, select the project from which to copy disclosure reasons, and then click **OK**.
 3. Click **OK** on the confirmation message.
9. After you are done configuring disclosure reasons, click **OK** to save the settings.

Disclosure Recipient List

If you have set up enhanced auditing for a project, each time users perform a document operation that could result in disclosure to another party, they are required to specify a reason for the disclosure of the information and who received it. (See "Disclosure Reason List" on the previous page for instructions to configure disclosure reasons.) You can configure your system to let users manually enter disclosure recipients or select them from a list of predefined values. You can also copy disclosure recipients from one project to another. This section describes how to configure disclosure recipient lists. After a disclosure recipient list is created, users can select values from it. If your enhanced auditing configuration allows it, as users manually enter disclosure recipients, they can be added to the list so others can use them. (See "Enhanced Auditing" on page 170 for instructions to configure enhanced auditing options.)

To configure disclosure recipients

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Projects**.
3. Expand the appropriate project, click **Enhanced Auditing**, and then do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Configure Disclosure Recipient Lists**.
 - On the toolbar, click **Configure Disclosure Recipient List**.
 - Right-click the selected item, and then click **Configure Disclosure Recipient Lists**.
 - On the right pane, double-click **Configure Disclosure Recipient List**.
4. In the **Disclosure Recipient List** dialog box, click **Add**.
5. In the box, type the disclosure recipients to appear in the list. Use a comma (,) to separate each recipient (for example, recipient1, recipient2, recipient3).
6. Click **OK** to save the disclosure recipients.
7. To remove a disclosure recipient from the list, select it, click **Remove**, and then click **Yes** to confirm the operation.
8. To copy disclosure recipients from another project, complete the following steps:
 1. Click **Copy**.
 2. From the list, select the project from which to copy disclosure recipients, and then click **OK**.
 3. Click **OK** on the confirmation message.
9. After you are done configuring disclosure recipients, click **OK** to save the settings..

Document Associations

When you set up document associations, users can view documents (across projects) that are associated with the document they have open. Documents are associated by a common index field, or index value that you specify and then link to another project in the document association. When a user searches for, and then views a document, they can also view all associated documents that meet the search criteria you defined in the document association for the project. When users view associated documents, the following search methods are used.

- When the document association is based on an index field, the index value in the document being viewed is used to search the index field configured in the associated project to find any documents with the same index value.
- When the document association is based on an index value (or wildcard), the value you specify is used to search the index field configured in the associated project to find documents with the same index value.

To access document association functions

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Projects**.
3. Expand the appropriate project, and then click **Document Associations**.
4. The right pane shows a list of existing document associations, and shows for each one the:
 - Identification number
 - Name for the document association
 - Project to which the document association is linked

As you work with document associations, see the following related sections for additional information:

- See "Add Document Associations" below for instructions to complete this task.
- See "Import Document Associations" on page 175 for instructions to complete this task.
- See "Refresh the Document Associations List" on page 175 for instructions to complete this task.
- See "Delete Document Associations" on page 175 for instructions to complete this task.
- See "Export Document Associations" on page 176 for instructions to complete this task.
- See "Edit Document Association Properties" on page 176 for instructions to complete this task.

Add Document Associations

When you set up document associations, users can view documents (across projects) that are associated with the document they have open. (See "Document Associations" on the previous page for information about the search methods that are used.) Documents are associated by a common index field, or index value that you specify and then link to another project in the document association. As an alternative to specifying a specific index field name or index value, you can assign wildcard characters as search criteria. (See "Search Criteria Guidelines" on page 346 for more information.)

After you create a document association that links one or more index fields, specific index values, or wildcard characters in one project to a second project, you can then create subsequent document associations for each project in your entity.

When you specify date search criteria for a document association, you can use the [CURRENTDATETIME] tag to represent the current date and time that the search is run. This is particularly useful when you need to identify documents that are of a certain age. A specified number of years (Y), months (M), days (D), hours (H), minutes (N), or seconds (S) can be added to or subtracted from the current date and time. Some examples of uses for the [CURRENTDATETIME] tag are shown in the following table.

This value	Equals
[CURRENTDATETIME]	Current date and time
[CURRENTDATETIME+1Y]	Current date and time plus one year
[CURRENTDATETIME-12M]	Current date and time minus 12 months
[CURRENTDATETIME+2D]	Current date and time plus two days
[CURRENTDATETIME-96H]	Current date and time minus 96 hours
[CURRENTDATETIME+900N]	Current date and time plus 900 minutes
[CURRENTDATETIME+120S]	Current date and time plus 120 seconds

To add document associations

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Projects**.
3. Expand the appropriate project, and then click **Document Associations**.
4. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **New Document Association**.
 - On the toolbar, click **New**.
 - Right-click the selected item, and then click **New Document Association**.
5. In the **Association Name** box, type a name to identify the document association.
6. From the **Search Project** list, select the project to be searched for the common criteria you specify.

 When users perform a search in the project where you are creating the document association, the project you select is also searched.
7. In the **Search Criteria** area, you can select an index field name from the list, type a specific index value in the field, or type wildcard characters as search criteria. (See "Search Criteria Guidelines" on page 346 for more information.)
8. From the **Search Type** list, select one of the following:
 - For your search to return any document that meets at least one of your index field search criteria, select **Or**.
 - For your search to return any document that meets all of your index field search criteria, select **And**.
9. From the **Sort By** list, select the index field by which to sort your search results.
10. (Optional) To test that your search criteria is valid, click **Test Criteria**, and then click **OK** on the message.
11. Click **OK** to save the document association.

Import Document Associations

You can import document associations that were previously exported into an XML file. (See "Export Document Associations" on the next page for instructions to complete this task.)

To import document associations

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Projects**.
3. Expand the appropriate project, and then click **Document Associations**.
4. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Import**.
 - On the toolbar, click **Import**.
 - Right-click the selected item, and then click **Import**.
5. In the **Import Document Association** dialog box, locate the document association file to import.
6. Select the document association file, and then click **Open**.
7. On the confirmation message, click **OK**.

Refresh the Document Associations List

To ensure the document associations list contains the most current information, you can manually refresh it.

To refresh the document associations list

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Projects**.
3. Expand the appropriate project, and then click **Document Associations**.
4. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Refresh**.
 - On the toolbar, click **Refresh**.
 - Right-click the selected item, and then click **Refresh**.

Delete Document Associations

You can delete document associations by performing the following procedure.

To delete document associations

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Projects**.
3. Expand the appropriate project, and then click **Document Associations**.
4. On the right pane, select the document associations to delete (hold down the Ctrl key to select multiple items).

5. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Delete**.
 - On the toolbar, click **Delete**.
 - Right-click the selected item, and then click **Delete**.
6. Click **Yes** to confirm the deletion.

Export Document Associations

You can export document associations into an XML file by performing the following procedure.

To export document associations

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Projects**.
3. Expand the appropriate project, and then click **Document Associations**.
4. On the right pane, select the document association to export.
5. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Export**.
 - On the toolbar, click **Export**.
 - Right-click the selected item, and then click **Export**.
6. In the **Export Document Association** dialog box, select the location where the export file will go.
7. In the **File Name** box, type a name for the export file, and then click **Save**.
8. Click **OK** on the confirmation message.

Edit Document Association Properties

You can edit document association properties by performing the following procedure.

To edit document association properties

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Projects**.
3. Expand the appropriate project, and then click **Document Associations**.
4. On the right pane, select the document association to edit.
5. Do one of the following:
 - Double-click the selected item.
 - On the **Action** menu, point to **All Tasks**, and then click **Properties**.
 - On the toolbar, click **Properties**.
 - Right-click the selected item, and then click **Properties**.
6. Edit the properties. (See "To add document associations" on page 174 for a description of the properties.)

7. (Optional) To test that your search criteria is valid, click **Test Criteria**, and then click **OK** on the message.
8. Click **OK** to save the document association.

Document Security Levels

In addition to project-level security, you can assign security at the document level. (See "Security Access" on page 188 for more information about project-level security.) Applying security at the document-level provides a more precise way to control access to information. After you define the criteria for a security level, you can automatically or manually apply it to documents. A document can have an unlimited number of security levels assigned to it. After security levels are applied to a document, it is no longer accessible to all users with security access to the project. Instead, to access that document users must also have access to at least one of the document security levels assigned to it.

To access document security levels functions

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Projects**.
3. Expand the appropriate project, and then click **Document Security Levels**.

The right pane shows a list of existing document security levels.

As you work with document security levels, see the following related sections for additional information:

- See "Add Document Security Levels" below for instructions to complete this task.
- See "Refresh the Document Security Levels List" on page 179 for instructions to complete this task.
- See "Apply Document Security Levels to Current Documents" on page 180 for instructions to complete this task.
- See "Submit Document Security Levels to be Applied to Current Documents" on page 180 for instructions to complete this task.
- See "Delete Document Security Levels" on page 181 for instructions to complete this task.
- See "Edit Properties for Document Security Levels " on page 181 for instructions to complete this task.

Add Document Security Levels

Document security levels contain "automatic selection criteria" that consists of index values that you specify. These index values are used to evaluate documents to determine whether the security level is applied to them. After automatic selection criteria is defined, you can choose when to apply document security levels. You can also choose to have the document security level automatically removed when index values are altered so they no longer match the defined selection criteria. These options are described in the following procedure. In addition to these options, after you add document security levels, you can also do the following:

- As an administrator, you can manually apply or remove document security levels to documents in PaperVision Enterprise. See the "Apply or Remove Document Security" topic in the online help or the *PaperVision Enterprise User Guide* for instructions. You can easily identify documents

that are assigned a document security level, as a lock displays in the **Status** column for the document.

- You can apply a security level to all existing documents in a project that meet the defined automatic selection criteria. See "Apply Document Security Levels to Current Documents" on page 180 for instructions.
- You can submit a security level to be applied to all existing documents in a project that meet the defined automatic selection criteria via a maintenance job that is run by the automation service. See "Submit Document Security Levels to be Applied to Current Documents" on page 180 for instructions.



T I P

To provide the greatest level of document security, first create a global document security level that restricts all document access, and then create individual document security levels that grant access to specific users. To create a global document security level, do not select any users or groups when you add the document security level.

To add document security levels

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Projects**.
3. Expand the appropriate project, and then click **Document Security Levels**.
4. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **New Document Security Level**.
 - On the toolbar, click **New**.
 - Right-click the selected item, and then click **New Document Security Level**.
5. On the **General** tab, in the **Level Name** box, type a name for the document security level.
6. In the **Grant Access to** area, select the users and groups who will have access to any document with this security level.
7. Do one of the following:
 - If you do not want to define index criteria for the document security level, click **OK** to save the document security level and complete this procedure.
 - To define index criteria for the document security level, click the **Criteria** tab, and then go to the next step in this procedure.
8. In the **Automatic Selection Criteria** area, type a specific index value or wildcard characters in the fields you want to define for selection criteria. (See "Search Criteria Guidelines" on page 346 for more information.)
9. From the **Search Type** list, select one of the following:
 - For your search to return any document that meets at least one of your index field search criteria, select **Or**.
 - For your search to return any document that meets all of your index field search criteria, select **And**.

10. In the **Automatic Selection Criteria Application** area, you can select the following options:
 - **Apply when new document index values meet criteria** - When selected, as documents are imported or added, the document security level is automatically applied to documents with index values that match what is defined in the **Automatic Selection Criteria** area.
 - **Apply when altered index values meet criteria** - When selected, as index values are changed so that they match what is defined in the **Automatic Selection Criteria** area, the document security level is automatically applied to the documents with matching index values.
 - **Remove when altered index values no longer meet criteria** - When selected, as index field values are changed so that they no longer match what is defined in the **Automatic Selection Criteria** area, the document security level is automatically removed from the documents with index values that no longer match.
11. (Optional) To test that your index criteria is valid, click **Test Criteria**, and then click **OK** on the message.
12. Click **OK** to save the document security level.
13. To apply the document security level to existing documents, you can use one of the following methods:
 - To immediately apply document security levels to existing documents, see "Apply Document Security Levels to Current Documents" on the next page for instructions to use this method.
 - To apply document security levels by submitting a maintenance job, see "Submit Document Security Levels to be Applied to Current Documents" on the next page for instructions to use this method.
 - To manually apply or remove document security levels to documents in PaperVision Enterprise. See the "Apply or Remove Document Security" topic in the online help or the *PaperVision Enterprise User Guide* for instructions.

Refresh the Document Security Levels List

To ensure the document security levels list contains the most current information, you can manually refresh it.

To refresh the document security levels list

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Projects**.
3. Expand the appropriate project, and then click **Document Security Levels**.
4. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Refresh**.
 - On the toolbar, click **Refresh**.
 - Right-click the selected item, and then click **Refresh**.

Apply Document Security Levels to Current Documents

Before you can submit document security levels for application to current documents, you must first add a document security level with automatic selection criteria defined. (See "Add Document Security Levels" on page 177 for instructions.) When you apply document security levels to current documents, all existing documents in a project are evaluated against the automatic selection criteria defined in the document security levels, and then document security levels are applied to the documents that match.

To apply document security levels to current documents

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Projects**.
3. Expand the appropriate project, and then click **Document Security Levels**.
4. On the right pane, select the document security level to apply to current documents.
5. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Apply to Current Documents**.
 - On the toolbar, click **Apply**.
 - Right-click the selected item, and then click **Apply to Current Documents**.

A message appears showing the number of additional documents to which the document security level was applied.

6. Click **OK** to clear the message.

Submit Document Security Levels to be Applied to Current Documents

Before you can submit document security levels for application to current documents, you must first add a document security level with automatic selection criteria defined. See "Add Document Security Levels" on page 177 for instructions. When you submit a document security level to be applied to current documents, a maintenance job is created that is run by the automation service. (See "Maintenance Queue" on page 44 for more information.) When the maintenance job is run, all existing documents in a project are evaluated against the automatic selection criteria defined in the document security levels you submitted, and then document security levels are applied to the documents that match.

To submit document security levels to be applied to current documents

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Projects**.
3. Expand the appropriate project, and then click **Document Security Levels**.
4. On the right pane, select the document security levels to submit to be applied to current documents (hold down the Ctrl key to select multiple items).
5. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Submit to be Applied to Current Documents**.

- On the toolbar, click **Submit to be Applied**.
 - Right-click the selected item, and then click **Submit to be Applied to Current Documents**.
6. Click **Yes** to confirm the operation.
A message appears confirming that the maintenance queue entries were created to apply the document security levels you selected to existing documents.
 7. Click **OK** to clear the message.

Delete Document Security Levels

You can delete document security levels by performing the following procedure. When you delete a document security level, it is removed from the documents to which it was applied.

To delete document security levels

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Projects**.
3. Expand the appropriate project, and then click **Document Security Levels**.
4. On the right pane, select the document security levels to delete (hold down the Ctrl key to select multiple items).
5. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Delete**.
 - On the toolbar, click **Delete**.
 - Right-click the selected item, and then click **Delete**.
6. Click **Yes** to confirm the deletion.

Edit Properties for Document Security Levels

You can edit properties for document security levels by performing the following procedure.

To edit properties for document security levels

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Projects**.
3. Expand the appropriate project, and then click **Document Security Levels**.
4. On the right pane, select the document security level to edit.
5. Do one of the following:
 - Double-click the selected item.
 - On the **Action** menu, point to **All Tasks**, and then click **Properties**.
 - On the toolbar, click **Properties**.
 - Right-click the selected item, and then click **Properties**.
6. Edit the properties. (See "To add document security levels" on page 178 for a description of the properties.)

7. (Optional) To test your search criteria, on the **Criteria** tab, click **Test Criteria**.
8. Click **OK** to save the document security level.

Integration Definitions

Integration definitions let users access documents in PaperVision Enterprise from any windows-based application. For example, suppose you have software that is used in a doctor's office to track medical records, you can configure an integration definition that lets users search for and view records stored in PaperVision Enterprise directly from their medical records software. As an administrator you can configure: the actions that start the integration process, which data to extract when calling the third-party application, which index field values are used to search for documents, and how search results are displayed.

Important Prerequisites

Integration definitions require the **PaperVision.net Integrator** to run. This tool is included in your installation in the **Digitech Systems** folder where PaperVision Enterprise is installed. To use integration definitions, you must complete the following tasks:

1. Add integration definitions. (See "Add Integration Definitions" on the facing page for instructions.)
2. In the **Digitech Systems** folder where your programs are installed, click **PaperVision.net Integrator** to run the setup wizard, and then follow the instructions on the screens to configure the **PaperVision.net Integrator**.
3. Ensure that the **PaperVision.net Integrator** is running when you want to use integration definitions.

If you selected the **Auto-Login** option when you ran the setup wizard, then the **PaperVision.net Integrator** automatically runs when a user logs into PaperVision Enterprise. If the user is not logged into PaperVision Enterprise, then the **PaperVision.net Integrator** must be started manually. After the **PaperVision.net Integrator** is started, it automatically retrieves the latest integration definitions.



T I P

Right-click the **PaperVision.net Integrator** icon in the Windows notification area at the bottom of your screen to access commands to log out and refresh integration definitions.

To access functions for integration definitions

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Projects**.
3. Expand the appropriate project, and then click **Integration Definitions**.
4. The right pane shows a list of existing integration definitions.

As you work with integration definitions, see the following related sections for additional information:

- See "Add Integration Definitions" on the facing page for instructions to complete this task.

- See "Import Integration Definitions" on page 186 for instructions to complete this task.
- See "Refresh the Integration Definitions List" on page 186 for instructions to complete this task.
- See "Delete Integration Definitions" on page 187 for instructions to complete this task.
- See "Export Integration Definitions" on page 187 for instructions to complete this task.
- See "Edit Properties for Integration Definitions" on page 188 for instructions to complete this task.

Add Integration Definitions

When you add an integration definition you specify information required for a third-party application to access documents in PaperVision Enterprise. You can configure: the actions that start the integration process, which data to extract when calling the third-party application, which index field values are used to search for documents, and how search results are displayed. After you add integration definitions, ensure that the **PaperVision.net Integrator** is configured. (See "Integration Definitions" on the previous page for more information.)



IMPORTANT

Make sure that the application from which you want to access PaperVision Enterprise is open and running before you add integration definitions.

To add integration definitions

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Projects**.
3. Expand the appropriate project, and then click **Integration Definitions**.
4. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **New Integration Definition**.
 - On the toolbar, click **New**.
 - Right-click the selected item, and then click **New Integration Definition**.
5. In the **Name** box, type a name for the integration definition.
6. In the **Method** list, select a method for starting the integration process and how it will extract data from the third-party application. Select one of the following options:
 - **Trigger on Hotkey; Enumerate Child Windows** - When selected, the integration process is started when a user presses the hot key sequence you specify while being on the "screen" you specify in the **Window Title** box. All of the information from the specified screen is extracted by listing the contents of all the child windows. Most items on a screen such as text boxes and labels are considered child windows.
 - **Trigger on Hotkey; Send Keys for Clipboard** - When selected, the integration process is started when a user presses the hot key sequence you specify while being on the "screen" you specify in the **Window Title** box. A predefined sequence of keystrokes you specify is sent to the third -party screen to copy specific data to the clipboard for extraction. This method is particularly useful for terminal emulation applications that do not use child windows.

- **Trigger on Clipboard** - When selected, the integration is started when a user copies data to the windows clipboard while being on the “screen” you specify in the **Window Title** box. The information on the clipboard is then extracted.



NOTE

Before going to the next step, make sure that the application from which you want to access PaperVision Enterprise is open and running. This causes the “screen names” from the application to appear in the **Window Title** list for you to select.

7. In the **Window Title** list, select or type the name of the screen that integrates with PaperVision Enterprise.



NOTE

Triggers are passed to PaperVision Enterprise only when the specified **Window Title** appears on the title of the screen in the third-party application. This value can include only a portion of the title for the screen. For example, you can specify “Notepad” for an application screen title of “Test.txt - Notepad.” To cause the trigger to occur from any running window, select **<Any Window Title>**; this is effective for applications that do not contain a constant value in their window titles.

8. If the **Method** you selected in step 6 includes hot keys, then perform the following sub-procedure to define the key sequence that will cause the integration to start. Otherwise, continue to the next step of the main procedure.



NOTE

You must define a hot key that is not already in use by the third-party application.

1. In the **Hotkey Setup** area, select the check box next to the key(s) you want to include (**Ctrl**, **Alt**, **Shift**).
 2. From the list, select the key that must be pressed in conjunction with the key(s) selected in the previous step.
9. If the **Method** you selected in step 6 is **Trigger on Hotkey; Send Keys for Clipboard**, then perform the following sub-procedure to define the key sequence needed to copy specific data from the third -party screen to the clipboard for extraction. Otherwise, continue to the next step of the main procedure.
 1. In the **Send Keys Configuration** area, click **Configure**.
 2. In the **Configure Send Keys** dialog box, click **Add**.
 3. In the **Add Key Sequences** dialog box, press each key combination as if you were doing them in the third-party application.

As you type, the values appear in the **Defined Key Sequence to Send** list.
 4. To cause a Tab to occur in the key sequence, click **Send <Tab>**.
 5. To cause a delay to occur in the key sequence, click **Insert Delay**, type the number of milliseconds to delay before performing the next key sequence, and then click **OK**.

**T I P**

Inserting time delays between keystrokes provides time for the third-party application to process input from PaperVision Enterprise.

6. After you are done specifying key sequences, on the **Add Key Sequences** dialog box, click **Finished**.
7. In the **Configure Send Keys** dialog box, click **Test**.
The specified key sequence is sent to the screen specified in the **Window Title** list and the raw data extracted from the application appears in the **View All Data** window.
8. Make any needed adjustments to correctly capture the data, and after you are satisfied with the results, click **OK**.
10. In the **Index Field Criteria** area, click **Configure**.
11. Select the index field to configure, and then click **Edit**.
12. From the **Parse Type** list, select one of the following values:
 - **Absolute Position** - When selected, the index field data is extracted from the third-party application based on the line and column position you specify.
 - **Regular Expression** - When selected, the index field data is extracted that meets the specified regular expression.
 - **Regular Expression/Position** - When selected, the first text occurrence of index field data that meets the specified regular expression is located. Then, the index field data is extracted based on the specified column position and the first character of the matching text.
13. If the selected **Parse Type** is **Regular Expression** or **Regular Expression/Position**, in the **Regular Exp** box, type the regular expression (See "Regular Expression Syntax and Metacharacters" on page 348 for more information.)
14. If the selected **Parse Type** is **Absolute Position** or **Regular Expression/Position**, then perform the following sub-procedure to define the position of the data. Otherwise, continue to the next step of the main procedure.
 1. Click **Configure**.
 2. In the **Configure Parsing** dialog box, select the data to extract for the index field search.
 3. Click **OK** to populate the **Line** and **Column** boxes.
 4. In the **Length** box, type the length of the index field value.
 5. In the **Configure Field Name** dialog box, click **Test Parsing**.
 6. Review the **Found Text** content, and then do one of the following:
 - If you are satisfied with the text found, click **OK** twice, and then continue to the next step of the main procedure.
 - If you are not satisfied with the text found, click **OK**, make any needed adjustments to correctly capture the data, and then click **Test Parsing**. Repeat testing and adjusting until you are satisfied with the results, click **OK** twice, and then continue to the next step of the main procedure.

15. Repeat steps 11-14 for any additional index field search criteria, and then click **OK** to save the configuration for index field criteria.
16. In the **New Integration Definition** dialog box, from the **Search Type** list, select one of the following:
 - For your search to return any document that meets at least one of your index field search criteria, select **Or**.
 - For your search to return any document that meets all of your index field search criteria, select **And**.
17. From the **Sort By** list, select the index field by which to sort your search results.
18. In the **Display Selection** area, select one of the following options:
 - **Search Results** - When selected, the results of the search are displayed.
 - **First Document** - When selected, the first document that matches the search criteria is displayed.
19. Click **Save**.

Import Integration Definitions

You can import integration definitions that were previously exported into an XML file (See "Export Integration Definitions" on the facing page for instructions to complete this task.)

To import integration definitions

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Projects**.
3. Expand the appropriate project, and then click **Integration Definitions**.
4. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Import**.
 - On the toolbar, click **Import**.
 - Right-click the selected item, and then click **Import**.
5. In the **Import Integration Definition** dialog box, locate the integration definition file to import.
6. Select the integration definition file, and then click **Open**.
7. On the confirmation message, click **OK**.

Refresh the Integration Definitions List

To ensure the integration definition list contains the most current information, you can manually refresh it.

To refresh the integration definitions list

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Projects**.
3. Expand the appropriate project, and then click **Integration Definitions**.

4. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Refresh**.
 - On the toolbar, click **Refresh**.
 - Right-click the selected item, and then click **Refresh**.

Delete Integration Definitions

You can delete integration definitions by performing the following procedure.

To delete integration definitions

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Projects**.
3. Expand the appropriate project, and then click **Integration Definitions**.
4. On the right pane, select the integration definitions to delete (hold down the Ctrl key to select multiple items).
5. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Delete**.
 - On the toolbar, click **Delete**.
 - Right-click the selected item, and then click **Delete**.
6. Click **Yes** to confirm the deletion.

Export Integration Definitions

You can export integration definitions into an XML file by performing the following procedure.

To export integration definitions

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Projects**.
3. Expand the appropriate project, and then click **Integration Definitions**.
4. On the right pane, select the integration definition to export.
5. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Export**.
 - On the toolbar, click **Export**.
 - Right-click the selected item, and then click **Export**.
6. In the **Export Integration Definition** dialog box, select the location where the export file will go.
7. In the **File Name** box, type a name for the export file, and then click **Save**.
8. Click **OK** on the confirmation message.

Edit Properties for Integration Definitions

You can edit properties for integration definitions by performing the following procedure.

To edit properties for integration definitions

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Projects**.
3. Expand the appropriate project, and then click **Integration Definitions**.
4. On the right pane, select the integration definition to edit.
5. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Properties**.
 - On the toolbar, click **Properties**.
 - Right-click the selected item, and then click **Properties**.
6. Edit the properties. (See "Add Integration Definitions" on page 183 for a description of the properties.)
7. Click **OK** to save the integration definition.

Security Access

Security access is applied at the project-level and assigned to users and groups. (See "System Users" on page 144 and "System Groups" on page 142 for instructions to create user accounts and groups.) Security access features let you limit access to projects, functionality, and specific fields. Security rights are cumulative, so users gain their assigned individual rights as well as those assigned to any groups of which they are a member. In addition to project-level security, you can also assign security at the document level. (See "Document Security Levels" on page 177 for more information.)

To access security access functions

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Projects**.
3. Expand the appropriate project, and then click **Security Access**.

The right pane shows a list of users and groups with defined security access.

As you work with document security levels, see the following related sections for additional information:

- See "Add Project Security Access" below for instructions to complete this task.
- See "Refresh the Security Access List" on page 191 for instructions to complete this task.
- See "Delete Security Access" on page 192 for instructions to complete this task.
- See "Edit Properties for Security Access" on page 192 for instructions to complete this task.

Add Project Security Access

Before you can assign security access, the users and groups to which you want to assign access must exist. (See "System Users" on page 144 and "System Groups" on page 142 for instructions to create user accounts and groups.) When you add security access, you can limit access to projects, functionality, and specific fields. These options are described in the following procedure.

**N O T E**

Security rights are cumulative, so users gain their assigned individual rights as well as those assigned to any groups of which they are a member.

To add new project security access

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Projects**.
3. Expand the appropriate project, and then click **Security Access**.
4. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **New Security Access**.
 - On the toolbar, click **New**.
 - Right-click the selected item, and then click **New Security Access**.
5. On the **General** tab, select the users and groups to receive security access to the project.

**N O T E**

If you select a user or group who already has rights in this project, they will be replaced with the new ones you are defining.

6. Click the **Rights** tab, and then do one of the following:
 - To assign all of the listed rights, click **All Rights** on the lower-left corner of the dialog box, and then go to step 14 to assign access to document fields.
 - To assign specific rights continue to the next step.
7. In the **Document Functions** area, select the functions to which you want to assign rights:
 - **View Documents** - When selected, the specified users can view documents.
 - **Save/Open Documents** - When selected, the specified users can save documents and open them in their native applications (as determined by their operating system).
 - **Add Documents** - When selected, the specified users can add documents.
 - **Print/Fax Documents** - When selected, the specified users can print and fax documents.
 - **View Outside PaperVision** - When selected, the specified users can open documents outside of PaperVision Enterprise by clicking the **Open** command from the PaperVision Viewer or Browser-Based Viewer.
 - **Tag for Migration** - When selected, the specified users can tag documents for migration.
 - **Modify Documents** - When selected, the specified users can alter document index values and check documents in and out of version control.
 - **Email Documents** - When selected, the specified users can send documents via email.
 - **View Workflow Status** - When selected, the specified users can view the status of Workflow instances for documents.
 - **Create Document Grants** - When selected, the specified users can share documents via a URL address.

- **Delete Documents** - When selected, the specified users can delete documents or move them to the Recycle Bin based on the **Recycle Bin Usage** settings for the project. (See the "To edit project properties" on page 162 procedure for a description of the Recycle Bin usage options.)
 - **Workflow Instantiations** - When selected, the specified users can create new WorkFlow instances for documents.
8. In the **Annotations** area, select the functions to which you want to assign rights:
- **View Annotations** - When selected, the specified users can view annotations on documents.
 - **Create/Modify Annotations** - When selected, the specified users can create and modify annotations on documents.
 - **Force Annotations On** - When selected, annotations always appear on documents, and are included when the document is saved, printed, or sent in an email message. The specified users can perform operations on documents to which they have access, but they cannot remove, hide, or move the annotations. For full-text documents with annotations forced on, full-text is hidden behind the annotation, but users can still perform a full-text search on the document. When this option is selected, users cannot modify the DPI resolution of PDF documents in the PaperVision Viewer settings so that the size and position of annotations on the document will not change.



NOTE

When **Force Annotations On** is selected, if an annotation fails to appear, the document will not appear to ensure that obscured information is not displayed. This method is enforced in PaperVision Enterprise, but there are extenuating circumstances outside of PaperVision Enterprise when a determined user might be able to view an annotated page without the annotation, thereby exposing any information hidden underneath the annotation.

9. In the **Audit Reviews** area, you can assign rights to the **For Individual Documents** function; when selected, the specified users can perform security audits on documents.
10. In the **Records Retention** area, select the functions to which you want to assign rights:
- **Apply Retention Locks** - When selected, the specified users can set document retention lock dates for records retention.
 - **Apply Destruction Dates** - When selected, the specified users can specify document destruction dates for records retention.
 - **Remove Retention Locks** - When selected, the specified users can clear document retention locks for records retention.
 - **Approve Destruction Lists** - When selected, the specified users can view and approve (or deny) scheduled document destruction lists for records retention.
11. In the **Folders** area, select the functions to which you want to assign rights:
- **View Folders** - When selected, the specified users can view all folders.
 - **Move Docs into Folders** - When selected, the specified users can move documents into folders.

- **Delete Folders** - When selected, the specified users can delete folders.
 - **Move Folders** - When selected, the specified users can move folders.
 - **Remove Docs from Folders** - When selected, the specified users can remove documents from folders.
 - **Create Folders** - When selected, the specified users can create new folders.
 - **Rename Folders** - When selected, the specified users can rename folders.
12. In the **Signatures** area, select the functions to which you want to assign rights:
 - **View Signatures** - When selected, the specified users can view signatures that are applied to documents.
 - **Sign Documents** - When selected, the specified users can electronically sign documents.
 13. In the **Recycle Bin** area, select the functions to which you want to assign rights:
 - **View Recycle Bin** - When selected, the specified users can view items in the Recycle Bin, and include recycled documents in project searches.
 - **Empty Recycle Bin** - When selected, the specified users can empty the Recycle Bin, permanently removing those items from the system.
 - **Restore Documents** - When selected, the specified users can move items out of the Recycle Bin and restore them to the project.
 14. Click the **Fields** tab.
 15. In the **Visible/Searchable Fields** area, clear the check boxes next to the fields that the specified users cannot view or search.
 16. If you selected the **Modify Documents** function on the **Rights** tab, in the **Editable Fields** area, clear the check boxes next to the fields that the specified users cannot modify.
 17. Click **OK**, and then click **Yes** on the confirmation message.

Refresh the Security Access List

To ensure the security access list contains the most current information, you can manually refresh it.

To refresh the security access list

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Projects**.
3. Expand the appropriate project, and then click **Security Access**.
4. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Refresh**.
 - On the toolbar, click **Refresh**.
 - Right-click the selected item, and then click **Refresh**.

Delete Security Access

You can delete security access by performing the following procedure.

To delete security access

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Projects**.
3. Expand the appropriate project, and then click **Security Access**.
4. On the right pane, select the users for which you want to delete security access (hold down the Ctrl key to select multiple items).
5. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Delete**.
 - On the toolbar, click **Delete**.
 - Right-click the selected item, and then click **Delete**.
6. Click **Yes** to confirm the deletion.

Edit Properties for Security Access

You can edit properties for security access by performing the following procedure.

To edit properties for security access

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Projects**.
3. Expand the appropriate project, and then click **Security Access**.
4. On the right pane, select the security access to edit.
5. Do one of the following:
 - Double-click the selected item.
 - On the **Action** menu, point to **All Tasks**, and then click **Properties**.
 - On the toolbar, click **Properties**.
 - Right-click the selected item, and then click **Properties**.
6. You can edit the properties on the **Rights** and **Fields** tabs. (See "To add new project security access" on page 189 for a description of the properties.)



NOTE

On the **General** tab, you cannot edit to whom the security access is applied.

7. Click **OK** to save the security access.

Directory Manager Jobs

You can automate the batch import of documents from any source media by using a directory manager job. Imported documents can be automatically indexed by the directory name the files reside in, the name of the file, a delimited segment of the file name, or the file modification date. This functionality provides a way to: pull in an organization's ad hoc document management system (using directories and file names), import documents scanned by a third-party application, and integrate with fax server software and network-attached scanners and photocopiers.

Active directory manager jobs are automatically run by the automation service when you configure a **Directory Manager Jobs** operation. (See "Configure Automation Service Scheduling" on page 61 for instructions.) As the directory manager job runs, the modification date of the files is compared to the minimum modification date specified in the job. Only files that fall on or after the minimum modification date (if enabled) are imported. After the import is complete, the minimum modification date that is stored for the job is automatically updated with the most recent modification date of any of the imported files. Files can be imported into a new data group (copied from their source location) or referenced at their source location.

Directory manager jobs can import image files that have full-text content. If a file with the same name and a **.PVFULLTEXT** extension (for example, **document.TIF** and **document.PVFULLTEXT**) exists in the same directory as the imported file, it is used to automatically populate the full-text data for that document. If the imported document contains multiple pages, the **PVFULLTEXT** file should use the Form Feed character (ASCII character 12) to separate pages within the document.

Global administrators can require that a marker file called **dirmgr.submit** must exist in the path before the directory manager job imports any of the files. (See "Data System Settings" on page 53 for instructions.) The content of the submit file is irrelevant, as it is not imported as part of the job. Checking for this file ensures that the directory manager does not run while files are being transmitted which can cause issues.

Directory manager jobs can also process PaperVision Package Files. See "About Directory Manager Jobs and PaperVision Package Files" on page 197 for more information.

To view directory manager jobs

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Projects**.
3. Expand the appropriate project, and then click **Directory Manager Jobs**.

The right pane shows for each directory manager job the:

- Name
- Status (active or inactive)
- Path monitored for incoming documents
- Workstation to import the documents

To add directory manager jobs

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Projects**.
3. Expand the appropriate project, and then click **Directory Manager Jobs**.

4. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **New Directory Manager Job**.
 - On the toolbar, click **New**.
 - Right-click the selected item, and then click **New Directory Manager Job**.
5. In the **Job Name** box, type a name for the directory manager job.
6. In the **Path** box, do one of the following:
 - Type the path to be monitored for incoming documents.
 - Click the ellipsis button, select the path to be monitored, and then click **OK** or **Save**.



NOTE

Do not set up jobs that could potentially import the same document more than once. For example, do not have multiple workstations monitor the same paths for the same file extensions.

7. In the **Workstation** area, do one of the following:
 - Select **Any** to allow any workstation or automation server to perform the import of documents.
 - Select **Specific** to assign a specific workstation or automation service, and then type or select a server name (for example, Server1) or workstation instance in the ServerName_Instance format (for example, Server1_12 would allow documents to be imported by instance number 12 on Server1).
8. In the **Minimum Modified Date** area, do one of the following:
 - Select **Disabled** to turn off the checking of file dates during import.
 - Select **Enabled**, and then type a date and time to specify that any documents with a modified date value greater than or equal to this value will be considered for import.
9. To extract index values from a delimited portion of the file name, in the **Field Delimiter** box, type the delimiter used to break the file name into segments. For example, the delimiter for a file named "Bob Smith_777-777-7777_October 12, 2017.TIF" is an underscore.
10. To create a field extraction, in the **Field Extraction** area, click **Add** to open the **Field Extraction** dialog box.
11. In the **Field Name** box, select the index field for which you want to extract a value.
12. In the **Field Source** box, select the source that will populate the index field.

E X A M P L E

To help you understand the items available in the **Field Source** list, here is an example. If you used:

- A **Path** value of F:\Test\Import\
- A **Field Delimiter** value of an underscore (_)
- And the following path and file name:
F:\Test\Import\Acme Corp\A132\Bob Smith_777-77-7777.TIF

It would produce the following values for the listed field sources:

File Date: Date the file was last modified

File Name with Extension: Bob Smith_777-77-7777.TIF

File Name without Extension: Bob Smith_777-77-7777

Entire File Path: F:\Acme Corp\A132\Bob Smith_777-77-7777.TIF

Directory Level 0: F:\Test\Import\

Directory Level 1: Acme Corp

Directory Level 2: A132

Directory Level 3 through 64: [Blank]

File Name Segment 1: Bob Smith

File Name Segment 2: 777-77-7777

File Name Segment 3 through 64: [Blank]

13. Click **OK** to add the index field extraction.
14. To add more index field extractions, repeat the previous four steps.
15. In the **File Extensions** area, do one of the following:
 - If most of the files in the job path have extensions that will be imported, select **Import all files except the extensions listed below**, and then, type any file extensions (separated by a comma or a space) that should not be imported.
 - If most of the files in the job path have extensions that will not be imported, select **Import only files with the extensions listed below**, and then, type any file extensions (separated by a comma or a space) that should be imported.
16. In the **Output Data Group** area, do one of the following:
 - To copy the imported files to a new attachment data group, select **Copy files to a new data group**. If you select this option, specify whether you want to delete the original files after they are successfully imported by selecting or clearing the **Delete Original files after successful import** check box.

- To reference the files in their current location, select **Use an in-line data group located at the job path**.
17. In the **Error Handling** area, specify what the system should do when it encounters documents that do not have all required index fields populated or files that it cannot process for some reason, such as an open file conflict. Do one of the following:
 - To cause the system to stop importing files when it encounters an error, select **Stop Importing**. If you select this option, specify whether you want to disable the job by selecting or clearing the **Disable job** check box.
 - To cause the system to skip the document and keep importing files when it encounters an error, select **Skip document and continue**. If you select this option, specify whether you want administrators to be notified of errors by selecting or clearing the **Email administrators document import errors** check box.
 18. To temporarily disable the directory manager job, clear the **Active** check box.
 19. Click **OK** to create the new directory manager job.

To refresh the directory manager jobs list

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Projects**.
3. Expand the appropriate project, and then click **Directory Manager Jobs**.
4. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Refresh**.
 - On the toolbar, click **Refresh**.
 - Right-click the selected item, and then click **Refresh**.

To delete directory manager jobs

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Projects**.
3. Expand the appropriate project, and then click **Directory Manager Jobs**.
4. On the right pane, select the directory manager jobs to delete (hold down the Ctrl key to select multiple items).
5. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Delete**.
 - On the toolbar, click **Delete**.
 - Right-click the selected item, and then click **Delete**.
6. Click **Yes** to confirm the deletion.

To edit properties for directory manager jobs

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Projects**.
3. Expand the appropriate project, and then click **Directory Manager Jobs**.
4. On the right pane, select the directory manager job to edit.

5. Do one of the following:
 - Double-click the selected item.
 - On the **Action** menu, point to **All Tasks**, and then click **Properties**.
 - On the toolbar, click **Properties**.
 - Right-click the selected item, and then click **Properties**.
6. Edit the properties. (See "To add directory manager jobs" on page 193 for a description of the properties.)
7. Click **OK** to save the directory manager job.

About Directory Manager Jobs and PaperVision Package Files

Directory manager jobs can also process PaperVision Package Files. PaperVision Package Files are compressed and optionally encrypted files that contain all of the files (in the appropriate directory structure) for one of the supported data group types and include a file extension of **PVPKG**. (See "Data Group Types for Import" on page 105 for a list of supported data group types.)

Package files are particularly useful when you need to:

- transport a data group with added security by using encryption.
- increase file transfer speeds by transferring one large file rather than hundreds or thousands of small files.

Package files use compression and optional encryption that are 100% compatible with the PKZIP 2.04g compression format and the WinZip 9.0 AES encryption format. Therefore, package files can be created using most popular ZIP compression tools. However, you can use the PaperVision Data Transfer Manager to completely automate the creation and transport of package files.

For a directory manager job, to import package files, they must include a package information file. This file is an additional unencrypted file embedded in the root of the package file.

- The name of the package information file is: **PackageFileName.pvpkginfo**
- The contents of the file are:

```
<?xml version="1.0"?>
<PVPACKAGEINFO>
  <ENTID>EntityIDHere</ENTID>
  <ENCRYPTKEYNAME>KeyNameHere</ENCRYPTKEYNAME>
</PVPACKAGEINFO>
```

As the directory manager job imports a package file, it follows this process:

1. The directory manager job extracts the package information file.
2. It determines if the package contents are encrypted by checking the **ENTID** and **ENCRYPTKEYNAME** values.

3. If **ENCRYPTKEYNAME** has a value, it retrieves the encryption key value that corresponds to the encryption key name and entity ID, and uses it to decrypt the remaining contents of the package.
4. The contents of the package file are extracted to the **Package Workspace** path defined under your global system settings. (See "Local System Settings" on page 60 for more information.)
5. After the contents of the package file are fully extracted, the directory manager operation places them in a new data group (regardless of how the **Output Data Group** options are set for the directory manager job) because they reside at a temporary location. In addition, the **Minimum Modified Date** setting for the directory manager job is ignored because file dates can be modified during the package creation or package extraction.
6. It uses the file name specified in **IMPORTFILE**, to determine the data group type, and then imports the data group.
7. After the package file is processed, the contents are removed from the local package workspace directory and the original location (regardless of how the **Delete original files after successful import** option is set for the directory manager job).

Records Destruction Lists

Records destruction lists are created when documents are identified by a destruction policy that specifies that the documents must be reviewed prior to destruction. (See "Add Records Retention Policy Sets" on page 204 for instructions to specify options for destruction policies.) Access to destruction lists is based on project security rights. (See "Add Project Security Access" on page 188 for instructions to assign access to destruction lists.)

Destruction lists can be accessed from the Administration Console and the user client. Authorized users can approve or deny the destruction of documents in the destruction list only from the user client. From the Administration Console, you cannot view the documents in the destruction list, and can work only at the list level. Administrators can delete destruction lists without the documents being approved or denied. In addition, you can run a cleanup process that updates the documents contained in destruction lists. For example, if a document in a destruction list is deleted before it is approved for destruction, it continues to appear on the list and prevents the destruction list from being automatically deleted. Running the cleanup process removes deleted documents from the list and recalculates the number of documents in each list. If the list no longer contains any documents, it is automatically deleted.

To view records destruction lists

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Projects**.
3. Expand the appropriate project, and then click **Records Destruction Lists**.

The right pane shows a list of defined records destruction lists and shows for each one the:

- ID number
- Date and time of creation
- Name of the policy set
- Name of the policy applied
- Number of documents in the list

To clean up records destruction lists



NOTE

When you clean up a records destruction list, the document count is recalculated, and any empty lists are automatically deleted.

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Projects**.
3. Expand the appropriate project, and then click **Records Destruction Lists**.
4. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Cleanup Lists**.
 - On the toolbar, click **Cleanup Lists**.
 - Right-click the selected item, and then click **Cleanup Lists**.
5. On the confirmation message, click **Yes**.

To refresh the records destruction list

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Projects**.
3. Expand the appropriate project, and then click **Records Destruction Lists**.
4. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Refresh**.
 - On the toolbar, click **Refresh**.
 - Right-click the selected item, and then click **Refresh**.

To delete records destruction lists

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Projects**.
3. Expand the appropriate project, and then click **Records Destruction Lists**.
4. On the right pane, select the records destruction list to delete (hold down the Ctrl key to select multiple items).
5. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Delete**.
 - On the toolbar, click **Delete**.
 - Right-click the selected item, and then click **Delete**.
6. Click **Yes** to confirm the deletion.

Records Retention Policy Sets

Records Retention Policy Sets let you schedule the automated retention or destruction of documents. Retention policies set a lock date and time before which documents cannot be deleted or emptied from the Recycle Bin. Destruction policies set a destruction date and time after which documents will be deleted if they are not locked. Whether documents are deleted or moved to the Recycle Bin during the destruction process is determined by the **Recycle Bin Usage** settings for the project. (See the "To edit project properties" on page 162 procedure for a description of the Recycle Bin usage options.) You can set destruction policies to require that documents are reviewed prior to destruction. If document reviews are required, you can specify that the document reviewers receive an email, and you can choose to include a link to the list of documents to be reviewed.

The automation service automatically performs records retention processing when you configure a **Records Retention** operation. (See "Configure Automation Service Scheduling" on page 61 for instructions.) The active records retention policy sets are processed for each project under each entity. Documents are evaluated against each policy in the order that they appear on the **Policies** tab. For retention policies, only documents that are not locked are evaluated. For destruction policies, only documents that are not marked for destruction or review are evaluated. After the documents are evaluated, the operation applies the retention (lock) or destruction (deletion) date and time to documents according to the criteria specified in the records retention policy set. Documents that have destruction (deletion) dates and times that are earlier than the current date and time are deleted.



IMPORTANT

Regardless of the destruction date and time, if a policy does not exist for a project, then destruction will not occur.



NOTE

The following procedures describe tasks you can perform for existing records retention policy sets. See "Add Records Retention Policy Sets" on page 204 for instructions to create records retention policy sets.

To view records retention policy sets

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Projects**.
3. Expand the appropriate project, and then click **Records Retention Policy Sets**.

The right pane shows a list of defined records retention policy sets and shows for each one the:

- ID number
- Name
- Number of defined policies
- Status (whether the policy set is active or superseded)
- Date and time of creation
- User name of the person who created it

To import records retention policy sets



NOTE

Before performing this procedure, make sure that you have a properly-formatted XML file that was created by exporting a records retention policy set. See "To export records retention policy sets to an XML file" on the next page for instructions.

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Projects**.
3. Expand the appropriate project, and then click **Records Retention Policy Sets**.
4. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Import**.
 - On the toolbar, click **Import**.
 - Right-click the selected item, and then click **Import**.
5. In the **Import Records Retention Policy Set** dialog box, select the XML file that contains the records retention policy set information, and then click **Open**.
6. Click **OK** in the confirmation message.

To refresh the records retention policy sets list

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Projects**.
3. Expand the appropriate project, and then click **Records Retention Policy Sets**.
4. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Refresh**.
 - On the toolbar, click **Refresh**.
 - Right-click the selected item, and then click **Refresh**.

To delete records retention policy sets



NOTE

You can delete active and superseded policy sets. When the active policy set is deleted, the most recent remaining policy set with the highest ID number becomes the active policy set.

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Projects**.
3. Expand the appropriate project, and then click **Records Retention Policy Sets**.
4. On the right pane, select the records retention policy set to delete (hold down the Ctrl key to select multiple items).
5. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Delete**.
 - On the toolbar, click **Delete**.

- Right-click the selected item, and then click **Delete**.
6. Click **Yes** to confirm the deletion.

To export records retention policy sets to an XML file

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Projects**.
3. Expand the appropriate project, and then click **Records Retention Policy Sets**.
4. On the right pane, select the records retention policy set to export.
5. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Export**.
 - On the toolbar, click **Export**.
 - Right-click the selected item, and then click **Export**.
6. In the **Export Records Retention Policy Set** dialog box, select the location where the export file will go.
7. In the **File Name** box, type a name for the export file, and then click **Save**.
8. Click **OK** in the confirmation message.

To edit properties for records retention policy sets



NOTE

Saving your changes causes the edited records retention policy set to become active and supersede existing policy sets. When you edit a records retention policy set, the original policy set is not overwritten so that a complete list of policy sets is maintained for auditing purposes.

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Projects**.
3. Expand the appropriate project, and then click **Records Retention Policy Sets**.
4. On the right pane, select the records retention policy set.
5. Do one of the following:
 - Double-click the selected item.
 - On the **Action** menu, point to **All Tasks**, and then click **Properties**.
 - On the toolbar, click **Properties**.
 - Right-click the selected item, and then click **Properties**.
6. In the **Records Retention Policy Set Properties** dialog box, make your changes. (See "Add Records Retention Policy Sets" on page 204 for a description of the options.)
7. On the **Policies** tab, you can select an existing policy, and then do one of the following:
 - Click **Edit** to open the policy properties where you can make changes. (See "Add Records Retention Policy Sets" on page 204 for a description of the options.)
 - Click **Remove**, and then click **Yes** to remove the policy.

- Click the arrow keys to reorder the policy in the list.

**N O T E**

Documents are evaluated against each policy in the order that they appear on the **Policies** tab.

8. When you are finished modifying the properties, click **OK** to save the changes and make the records retention policy set active.

To clear document destruction or lock information

**T I P**

This feature is useful when documents were evaluated by a records retention policy set that contained incorrect information. For example, suppose a destruction time was incorrectly specified. Clearing the destruction information removes the erroneous destruction time so that the documents can be evaluated again after the policy is corrected.

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Projects**.
3. Expand the appropriate project, and then click **Records Retention Policy Sets**.
4. On the right pane, select the records retention policy set.
5. Do one of the following:
 - Double-click the selected item.
 - On the **Action** menu, point to **All Tasks**, and then click **Properties**.
 - On the toolbar, click **Properties**.
 - Right-click the selected item, and then click **Properties**.
6. On the **General** tab, from the **Clear** list, select one of the following values:
 - **Destruction Information** - When selected, all destruction dates, destruction information, and destruction lists for all documents in the project will be cleared so that no destruction is scheduled for any documents.
 - **Lock Information** - When selected, all lock dates and lock information for all documents in the project will be cleared so that no locks are maintained for any documents.
 - **Destruction and Lock Information** - When selected, all destruction dates, destruction information, destruction lists, lock dates, and lock information for all documents in the project will be cleared so that no destruction is scheduled or locks maintained for any documents.

**N O T E**

After the clear process is run once, the **Clear** list value resets to **Nothing** to specify that no destruction or retention information should be cleared when the corrected policy set is processed.

7. Click **OK** to save the changes and make the records retention policy set active.



NOTE

When you save the records retention policy set, a maintenance job to apply the most recent policy set appears on the **Maintenance Queue**. As long as a **Maintenance Queue** operation is scheduled, the policy changes will process quickly. This allows your changes to go into effect without having to wait for the **Records Retention Automated Operation** to run, as it likely does not run as frequently. (See "Configure Automation Service Scheduling" on page 61 for more information.)

Add Records Retention Policy Sets

This content describes how to create new records retention policy sets. See "Records Retention Policy Sets" on page 200 for instructions for tasks you can perform for existing records retention policy sets. Records retention policy sets contain settings and policies that define which documents should be retained and which ones should be destroyed.

The automation service automatically performs records retention processing when you configure a **Records Retention** operation. When you save the records retention policy set, a maintenance job to apply the most recent policy set appears on the **Maintenance Queue**. As long as a **Maintenance Queue** operation is scheduled, the policy changes will process quickly. This allows your changes to go into effect without having to wait for the **Records Retention Automated Operation** to run, as it likely does not run as frequently. (See "Configure Automation Service Scheduling" on page 61 for instructions to configure these operations.)

Each records retention policy set contains the following tabs:

- **General** - On this tab, you specify a name for the records retention policy set and any comments you want to include.
- **Policies** - On this tab, you can add, edit, remove and order policies. Each records retention policy set must have at least one policy defined. A policy defines criteria used to evaluate documents. Documents are evaluated against each policy in the order that they appear on the **Policies** tab. When a document meets all of the defined criteria, then the action specified by the policy is taken. After a document is locked or marked for destruction, it is no longer evaluated against any subsequent policies of the same type (retention or destruction). Whether documents are deleted or moved to the Recycle Bin during the destruction process is determined by the **Recycle Bin Usage** settings for the project. (See the "To edit project properties" on page 162 procedure for instructions to set the Recycle Bin usage options.)

Only one policy set can be active at a time. Each time a policy set is saved, the newly-saved policy set is activated, and any existing policy sets are superseded. Existing policy sets are not overwritten so that a list of policy sets is maintained for auditing. Each destruction or retention schedule references the policy and policy set name that was used to mark the document for destruction or retention.



NOTE

Clicking **OK** on the **New Records Retention Policy Set** dialog box causes the new records retention policy set to become active and supersede existing policy sets. Therefore, ensure that you define all criteria before saving.

To add records retention policy sets

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Projects**.
3. Expand the appropriate project, and then click **Records Retention Policy Sets**.
4. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **New Records Retention Policy Set**.
 - On the toolbar, click **New**.
 - Right-click the selected item, and then click **New Records Retention Policy Set**.
5. In the **New Records Retention Policy Set** dialog box, click the **General** tab.
6. In the **Policy Set Name** box, type a name for the policy set.
7. In the **Comments** box, type any information to include.
8. In the **Clear** list, you can specify if you want to clear document destruction or lock information from documents that have already been evaluated by the policy set. For new policies, set this value to **Nothing**. (See "To clear document destruction or lock information" on page 203 for information about the other options.)
9. Click the **Policies** tab.
10. Click **Add** to open the **New Policy** dialog box.
11. Click the **General** tab.
12. In the **General** area, you can set the following options:
 - **Policy Name** - This setting specifies the name of the policy within the records retention policy set.
 - **Status** - This setting specifies whether the policy is active. Inactive policies are not used to evaluate documents.
 - **Policy Type** - This setting specifies whether documents will be evaluated for destruction (deleted) or retention (locked). Choose one of the following options:
 - **Destruction** - Destruction policies set a destruction date and time after which documents will be deleted if they are not locked. Whether documents are deleted or moved to the Recycle Bin during the destruction process is determined by the **Recycle Bin Usage** settings for the project. (See the "To edit project properties" on page 162 procedure for instructions to set the Recycle Bin usage options.) For destruction policies, only documents that are not marked for destruction or review are evaluated.
 - **Retention** - Retention policies set a lock date and time before which documents cannot be deleted or emptied from the Recycle Bin. For retention policies, only documents that are not locked are evaluated. If you select this option, go to step 15 of this procedure.

13. To send email notifications when documents are scheduled for destruction, in the **Notifications** area, select the check box, and then in the **Email Address(es)** box, type the email addresses for the recipients; use commas to separate multiple addresses.



NOTE

The email notification is sent either when the automated policy processing or the document review process sets the destruction date/time for the document.

14. In the **Destruction Review** area, select one of the following options:
 - **Automatically destroy documents** - When selected, the destruction date/time is set for documents without any review process.
 - **Require document review prior to destruction** - When selected, documents are placed on a destruction list where they must be reviewed and then confirmed or denied for destruction. Access to destruction lists is based on project security rights. Destruction lists can be accessed from the Administration Console and the user interface. (See "Records Destruction Lists" on page 198 for more information.) If you select this option, you can specify the following items:
 - **Email Addresses** - If document reviews are required, you can specify that the document reviewers receive an email. In the **Email Address(es)** box, type the email addresses for the reviewers; use commas to separate multiple addresses.
 - **List Link URL** - In the email to reviewers, you can include a URL to the list of documents to be reviewed by typing it in this box. For example, this URL specifies the base URL to the web interface <https://login.imagesilo.com/>.
 - **Reviewer specifies destruction schedule** - When selected, the destruction date/time for documents will not automatically be calculated, but will be explicitly specified by the reviewer.
15. In the **Destruction Offset** or **Lock Offset** area, specify the event from which the calculation of destruction or lock dates will begin. In the third box, select one of the following options:
 - **after documents are identified** - When selected, the destruction or lock date/time is determined by adding the destruction or lock offset time to the time when documents that met the specified criteria were identified.
 - **from document creation date/time** - When selected, the destruction or lock date/time is determined by adding the destruction or lock offset time to the time the document first entered the system.
 - **after destruction is approved** - When selected, the destruction date/time is determined by adding the destruction or lock offset time to the time when the document reviewer approves destruction of the documents.
16. In the **Destruction Offset** or **Lock Offset** area, specify the amount of time you want to elapse from the event selected in the previous step to determine the destruction or lock date/time. In the first box, type the amount of time, and in the second box, select the unit of measure for the time.
17. Click the **Criteria** tab.

18. In the **Selection Criteria** area, type a specific index value or wildcard characters in the fields you want to define for selection criteria. (See "Search Criteria Guidelines" on page 346 for more information.)
19. From the **Search Type** list, select one of the following:
 - For your search to return any document that meets at least one of your index field search criteria, select **Or**.
 - For your search to return any document that meets all of your index field search criteria, select **And**.
20. (Optional) To test that your index criteria is valid, click **Test Criteria**, and then click **OK** on the message.
21. Click **OK** to save the records retention policy set.

This page was intentionally inserted without content.



CHAPTER 7

Message Manager

Message Manager Overview	210
Message Capture File Sets Overview	210
Message Capture Policy Sets	212



Message Manager Overview

The PaperVision Message Manager product is an optional, separately-licensed component that processes email messages to prepare them for storage in PaperVision Enterprise. When coupled with PaperVision WorkFlow, it can provide comprehensive customer service solutions. Message Manager can process email messages from Microsoft Exchange as well as most LINUX or UNIX email systems and offers the following components.

- **PaperVision Harvester** - This stand-alone desktop application can process messages directly from Outlook PST files or Exchange mailboxes. Harvester never removes messages from the PST files or Exchange mailboxes.
- **PaperVision Message Capture Server** - This Windows service processes messages from directories containing journaled messages. Any messages that exist in the monitored directories are removed once they are evaluated.

You can set policies that define parameters for how email messages are handled by the components listed above. (See "Message Capture Policy Sets" on page 212 for more information.) As email messages are processed, they are parsed into manageable pieces of data called Message Capture File Sets that are appended to data groups. (See "Message Capture File Sets Overview" below for information about the contents of Message Capture File Sets.) For Message Capture File Sets that are already in the system, see "Message Capture File Sets" on page 119 to access instructions for tasks you can perform.

Message Capture File Sets Overview

As the PaperVision Message Manager processes email messages, they are parsed into manageable pieces of data called Message Capture File Sets that are appended to data groups. You can set policies that define parameters for how email messages are handled. (See "Message Capture Policy Sets" on page 212 for more information.) Message Capture File Sets are specific to each entity. Message Capture File Sets are imported using the same process for importing data groups. (See "Import Data Groups" on page 101 for instructions.)

See "Message Capture File Sets" on page 119 to access instructions for tasks you can perform for the Message Capture File Sets that are already in the system. The primary value of Message Capture File Sets is the ability to perform a "roll back," which deletes the data it contains. This function is useful to remove Message Capture File Sets created by an incorrectly-configured job without affecting the rest of the information in the data group. (See "Roll Back Message Capture File Sets" on page 123 for more information about this function.)

Each Message Capture File Set contains at least the following files:

- **Data File(s)** - These files contain the output message data. They are named with a .PVMSGDATx extension.
- **Offset File(s)** - These files contain the offset data that is used to calculate where specific message data can be located within the corresponding data file. They are named with a .PVMSGOFFx extension.
- **Message File** - This file contains the document index values and the file set message numbers for each message. It is named with a .PVMSGDOC extension.

- **Info File** - This file contains the XML document describing the file set and summary information. It is named with a .PVMSGINFO extension.
- **Submit File** - The contents of this file are unimportant, as the existence of this file is used to trigger the import of the file set. It is named with a .SUBMIT extension. The .PVMSGSUBMIT file is generated when Message Manager closes the file set and it is ready to be imported into PaperVision Enterprise.

Non-Repudiation Process

As email messages are processed into file sets, a hash value is calculated and then stored for each message. When a user retrieves a message, the message hash value is recalculated against the retrieved message, and then verified against the stored hash value to validate that the message has not been tampered with.

Document Indexing

Regardless of project configuration, the following index values are always extracted from email messages. When the Message Capture File Sets are imported into PaperVision Enterprise, the import process expects the project fields to be named exactly as shown below.

- Sender
- Recipient
- Subject
- Message ID
- Message File Type
- Message Type
- Message Date/Time
- Message Size
- Message Attachment Name
- Message Encryption
- Message Priority
- Message Sensitivity
- Message Importance
- Message Source
- Message Envelope Journal
- Classification
- Capture Policy
- Capture Date/Time

During the import process, if some or all of the index fields do not exist within the project, those index fields are skipped. The index fields can be added at a later date, and the file set re-imported to populate the fields. Additionally, not every email message will contain all of the specified index fields.



NOTE

The Subject field is always truncated to a maximum of 900 characters due to a Microsoft SQL Server limitation of 900 bytes/characters in a database index.

Message Capture Policy Sets

Message Capture Policy Sets define which email messages should be retained and how. Only one policy set can be active at a given time. As new policy sets are saved, they are activated and supersede existing policy sets. The policy set name and ID used to create the content of each Message Capture File Set is recorded for auditing purposes. (See "Message Capture File Sets" on page 119 for instructions to access this information.)



NOTE

The following procedures describe tasks you can perform for existing Message Capture Policy Sets. See "Add Message Capture Policies" on page 214 for instructions to create new Message Capture Policy Sets.

To view Message Capture Policy Sets

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Message Capture Policy Sets**.

The right pane shows a list of defined Message Capture Policy Sets and shows for each one the:

- ID number
- Name
- Number of defined policies
- Status (whether the policy set is active or superseded)
- Date and time of creation
- User name of the person who created it

To import Message Capture Policy Sets



NOTE

Before performing this procedure, make sure that you have a properly-formatted XML file that was created by exporting a Message Capture Policy Set. See "To export Message Capture Policy Sets to an XML file" on the facing page for instructions.

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Message Capture Policy Sets**.

3. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Import**.
 - On the toolbar, click **Import**.
 - Right-click the selected item, and then click **Import**.
4. In the **Import Message Capture Policy Set** dialog box, select the XML file that contains the Message Capture Policy Set information, and then click **Open**.
5. Click **OK** in the confirmation message.

To refresh the Message Capture Policy Sets list

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Message Capture Policy Sets**.
3. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Refresh**.
 - On the toolbar, click **Refresh**.
 - Right-click the selected item, and then click **Refresh**.

To delete Message Capture Policy Sets

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Message Capture Policy Sets**.
3. On the right pane, select the Message Capture Policy Set(s) to delete (hold down the Ctrl key to select multiple items).
4. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Delete**.
 - On the toolbar, click **Delete**.
 - Right-click the selected item, and then click **Delete**.
5. Click **Yes** to confirm the deletion.

To export Message Capture Policy Sets to an XML file

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Message Capture Policy Sets**.
3. On the right pane, select the Message Capture Policy Set to export.
4. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Export**.
 - On the toolbar, click **Export**.
 - Right-click the selected item, and then click **Export**.
5. In the **Export Message Capture Policy Set** dialog box, select the location where the export file will go.
6. In the **File Name** box, type a name for the export file, and then click **Save**.

To edit properties for Message Capture Policy Sets



NOTE

Saving your changes causes the edited Message Capture Policy Set to become active and supersede existing policy sets.

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Message Capture Policy Sets**.
3. On the right pane, select the Message Capture Policy Set.
4. Do one of the following:
 - Double-click the selected item.
 - On the **Action** menu, point to **All Tasks**, and then click **Properties**.
 - On the toolbar, click **Properties**.
 - Right-click the selected item, and then click **Properties**.
5. In the **Message Capture Policy Set Properties** dialog box, make your changes. (See "Add Message Capture Policies" below for a description of the options.)
6. On the **Policies** tab, you can select an existing policy, and then do one of the following:
 - Click **Edit** to open the policy properties where you can make changes. (See "Add Message Capture Policies" below for a description of the options.)
 - Click **Remove**, and then click **Yes** to remove the policy.
 - Click the arrow keys to reorder the policy in the list.



NOTE

Email messages are evaluated against each policy in the order that they appear on the **Policies** tab.

7. When you are finished modifying the properties, click **Save** to save the changes and make the Message Capture Policy Set active.

Add Message Capture Policies

Message Capture Policy Sets contain settings and policies that define which email messages should be retained and how. (See "Message Capture Policy Sets" on page 212 for instructions for tasks you can perform for existing Message Capture Policy Sets.) Each Message Capture Policy Set contains the following tabs:

- **General** - On this tab, you specify a name for the Message Capture Policy Set and any comments you want to include.
- **Policies** - On this tab, you can add, edit, remove and order policies. Each Message Capture Policy Set must have at least one policy defined. A policy defines criteria used to evaluate each email message. Email messages are evaluated against each policy in the order that they appear on the **Policies** tab. When an email message meets all of the defined criteria, then the action specified by the policy is taken. If the action specified by a policy is **Drop** and the email message

meets all of its defined criteria, then the email message is not evaluated against any subsequent policies.

- **File Set Options** - On this tab, you specify limits for Message Capture File Sets and whether you want them encrypted, compressed, and processed through the full-text engine.



N O T E

As you add policies, keep in mind that clicking **Save** on the **New Message Capture Policy Set** dialog box causes the new Message Capture Policy Set to become active and supersede existing policy sets. Therefore, ensure that you define all criteria before saving.

To specify general options

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Message Capture Policy Sets**.
3. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **New Message Capture Policy Set**.
 - On the toolbar, click **New**.
 - Right-click the selected item, and then click **New Message Capture Policy Set**.
4. In the **New Message Capture Policy Set** dialog box, click the **General** tab.
5. In the **Policy Set Name** box, type a name for the policy set.
6. In the **Comments** box, type any information to include.

To add policies

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Message Capture Policy Sets**.
3. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **New Message Capture Policy Set**.
 - On the toolbar, click **New**.
 - Right-click the selected item, and then click **New Message Capture Policy Set**.
4. In the **New Message Capture Policy Set** dialog box, click the **Policies** tab.
5. Click **Add** to open the **New Policy** dialog box.
6. For information about the options on each tab, see the following:
 - See "General Settings" on the next page for instructions to set options on the **General** tab.
 - See "Message Settings" on page 217 for instructions to set options on the **Message** tab.
 - See "Sender Settings" on page 219 for instructions to set options on the **Sender** tab.
 - See "Recipient Settings" on page 220 for instructions to set options on the **Recipient** tab.

To specify file set options

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Message Capture Policy Sets**.

3. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **New Message Capture Policy Set**.
 - On the toolbar, click **New**.
 - Right-click the selected item, and then click **New Message Capture Policy Set**.
4. In the **New Message Capture Policy Set** dialog box, click the **File Set Options** tab.
5. You can set the following options:
 - **Max. Messages per File Set** - This option specifies the maximum number of email messages that is included in each Message Capture File Set. When this number is reached, a new Message Capture File Set is created.
 - **Max File Set Size (MB)** - This option specifies the maximum size in MB for each Message Capture File Set. When this size is reached, a new Message Capture File Set is created.
 - **Max. Inactive Minutes** - This option specifies the maximum number of minutes that the agent can sit idle (waiting for new messages) before a new Message Capture File Set is created.
 - **Message Encryption Key** - This option specifies whether encryption is applied to messages as they are stored in the Message Capture File Set. To apply encryption, from the list, select the encryption key. (If you need to add an encryption key, see "Encryption Keys" on page 135 for instructions.)
 - **Compress Messages** - If selected, messages are compressed before they are saved to the Message Capture File Set.
 - **Full-Text Import** - If selected, during the import process, messages are loaded into the full-text database which lets you perform full-text searches on the information.

General Settings

This content describes how to set the general options for a Message Capture Policy. Many of the values you specify, such as the policy name, status, mode, effective date, and action appear on the **Policies** tab and help you identify each policy defined for a Message Capture Policy Set.

To set the general options for a Message Capture Policy

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Message Capture Policy Sets**.
3. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **New Message Capture Policy Set**.
 - On the toolbar, click **New**.
 - Right-click the selected item, and then click **New Message Capture Policy Set**.
4. In the **New Message Capture Policy Set** dialog box, click the **Policies** tab.
5. Click **Add** to open the **New Policy** dialog box.
6. On the **General** tab, you can set the following options:
 - **Policy Name** - This setting specifies the name of the policy within the Message Capture Policy Set.

- **Effective Date** - This setting specifies the earliest date and time that the policy becomes effective to evaluate email messages.
- **Capture Mode** - This setting specifies which agents will use this policy. (See "Message Manager Overview" on page 210 for information about the agents.) You can choose one of the following options:
 - **All** - Select this option for the **PaperVision Harvester** and the **PaperVision Message Capture Server** to use this policy.
 - **Capture** - Select this option for only the **PaperVision Message Capture Server** to use this policy.
 - **Harvest** - Select this option for only the **PaperVision Harvester** to use this policy.
- **Action** - This setting specifies what action occurs when an email message meets the specified criteria. You can choose one of the following options:
 - **Capture** - Select this option to write the message to the Message Capture File Set for the specified project, and then stop evaluating the message against any additional policies.
 - **Capture and Continue** - Select this option to write the message to the Message Capture File Set for the specified project, and then continue to evaluate the message against any additional policies.
 - **Drop** - Select this option to ignore the message (that is, it is not written to the Message Capture File Set), and then stop evaluating the message against any additional policies.
- **Project** - The setting specifies the project where messages are written when they are captured.
- **Classification** - The setting specifies a hard-coded index field value of "Classification" that will contain the specified index field value when the messages is captured.
- **All Messages** - When selected, all messages evaluated against this policy will automatically meet its requirements. Therefore, when this option is selected, you cannot configure message, sender, or recipient settings for the policy.
- **Active** - When selected, the policy is active. When this option is cleared, the policy is inactive and messages are not evaluated against it.

Message Settings

This content describes how to set the message options for a Message Capture Policy. Message settings let you define evaluation options for the content, status, type, attachments, size, and encryption status of email messages.

To set the message options for a Message Capture Policy

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Message Capture Policy Sets**.
3. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **New Message Capture Policy Set**.
 - On the toolbar, click **New**.
 - Right-click the selected item, and then click **New Message Capture Policy Set**.

4. In the **New Message Capture Policy Set** dialog box, click the **Policies** tab.
5. Click **Add** to open the **New Policy** dialog box.
6. Click the **Message** tab, where you can set the following options:
 - **Subject Content** - This setting is a regular expression that specifies the subject content of the message that must be matched to meet the criteria for the policy. (See "Regular Expression Syntax and Metacharacters" on page 348 for more information about regular expressions.)
 - **Body Content** - This setting is a regular expression that specifies the body content of the message that must be matched to meet the criteria for the policy. (See "Regular Expression Syntax and Metacharacters" on page 348 for more information about regular expressions.)
 - **Message Sensitivity** - This setting specifies the message sensitivity that must be matched to meet the criteria for the policy. This value is not a regular expression, nor is it case-sensitive.
 - **Message Priority** - This setting specifies the message priority that must be matched to meet the criteria for the policy. This value is not a regular expression, nor is it case-sensitive.
 - **Message Importance** - This setting specifies the message importance that must be matched to meet the criteria for the policy. This value is not a regular expression, nor is it case-sensitive.
 - **Message Type** - This setting specifies the message type that must be matched to meet the criteria for the policy. This value is not a regular expression, nor is it case-sensitive.
 - **Attachment Name** - This setting is a regular expression that specifies an attachment name for the message that must exist to meet the criteria for the policy. (See "Regular Expression Syntax and Metacharacters" on page 348 for more information about regular expressions.)
 - **Attachment Exists** - This setting specifies whether the existence of an attachment is used to meet the criteria for the policy. You can choose one of the following options:
 - **<blank>** - Select this option to specify that the existence of message attachments is not evaluated.
 - **True** - Select this option to specify that the message must have an attachment.
 - **False** - Select this option to specify that the message must not have an attachment.
 - **Message Size** - This setting specifies the message size in bytes used to meet the criteria for the policy. From the list, you can choose one of the following options:
 - **>=** - Select this option to specify that the message size must be greater than or equal to the value you type in the next box.
 - **<=** - Select this option to specify that the message size must be less than or equal to the value you type in the next box.
 - **Message is Encrypted** - This setting specifies whether the encryption of a message is used to meet the criteria for the policy. You can choose one of the following options:
 - **<blank>** - Select this option to specify that message encryption is not evaluated.
 - **True** - Select this option to specify that the message must be encrypted.
 - **False** - Select this option to specify that the message must not be encrypted.

Sender Settings

This content describes how to set the sender options for a Message Capture Policy. Sender settings let you add, import, and delete sender addresses and active directory group names. The **Sender** tab contains the following two areas:

- **Sender Addresses** - This area shows a list of regular expressions against which messages are evaluated. If the email address of the sender meets the criteria of one of the regular expressions, the message is considered to have met the criteria specified.
- **Sender Active Directory Group Names** - This area shows a list of active directory group names. The list is not case sensitive. When defined, the sender email address of each message is evaluated against an active directory look up to determine whether it exists within a specified group. If it exists in one of the listed groups, the message is considered to have met the criteria specified.

To set sender addresses for a Message Capture Policy

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Message Capture Policy Sets**.
3. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **New Message Capture Policy Set**.
 - On the toolbar, click **New**.
 - Right-click the selected item, and then click **New Message Capture Policy Set**.
4. In the **New Message Capture Policy Set** dialog box, click the **Policies** tab.
5. Click **Add** to open the **New Policy** dialog box.
6. Click the **Sender** tab.
7. Under the **Sender Addresses** area, you can use the following options:
 - **Add** - Click this option to define sender addresses. In the **Add Sender Address** dialog box, type the regular expression that specifies a sender address, and then click **OK**. (See "Regular Expression Syntax and Metacharacters" on page 348 for more information about regular expressions.)
 - **Import** - Click this option to import a line-delimited list of addresses from a file. In the **Import Sender Address File** dialog box, select the file that contains the sender addresses, and then click **Open**.
 - **Delete** - Select the sender address(es) to delete (hold down the Ctrl key to select multiple items), and then click **Delete**. Click **Yes** to confirm the deletion.

To set sender active directory group names for a Message Capture Policy

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Message Capture Policy Sets**.
3. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **New Message Capture Policy Set**.
 - On the toolbar, click **New**.
 - Right-click the selected item, and then click **New Message Capture Policy Set**.

4. In the **New Message Capture Policy Set** dialog box, click the **Policies** tab.
5. Click **Add** to open the **New Policy** dialog box.
6. Click the **Sender** tab.
7. Under the **Sender Active Directory Group Names** area, you can use the following options:
 - **Add** - Click this option to define sender active directory group names. In the **Add Sender Group** dialog box, type the group name (not case sensitive), and then click **OK**.
 - **Import** - Click this option to import a line-delimited list of group names from a file. In the **Import Sender Group Names File** dialog box, select the file that contains the group names, and then click **Open**.
 - **Delete** - Select the group name(s) to delete (hold down the Ctrl key to select multiple items), and then click **Delete**. Click **Yes** to confirm the deletion.

Recipient Settings

This content describes how to set the recipient options for a Message Capture Policy. Recipient settings let you add, import, and delete recipient addresses and active directory group names. The **Recipient** tab contains the following two areas:

- **Recipient Addresses** - This area shows a list of regular expressions against which messages are evaluated. If the email address of the recipient meets the criteria of one of the regular expressions, the message is considered to have met the criteria specified.
- **Recipient Active Directory Group Names** - This area shows a list of active directory group names. The list is not case sensitive. When defined, the recipient email address of each message is evaluated against an active directory look up to determine whether it exists within a specified group. If it exists in one of the listed groups, the message is considered to have met the criteria specified.

To set recipient addresses for a Message Capture Policy

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Message Capture Policy Sets**.
3. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **New Message Capture Policy Set**.
 - On the toolbar, click **New**.
 - Right-click the selected item, and then click **New Message Capture Policy Set**.
4. In the **New Message Capture Policy Set** dialog box, click the **Policies** tab.
5. Click **Add** to open the **New Policy** dialog box.
6. Click the **Recipient** tab.
7. Under the **Recipient Addresses** area, you can use the following options:
 - **Add** - Click this option to define recipient addresses. In the **Add Recipient Address** dialog box, type the regular expression that specifies a recipient address, and then click **OK**. (See "Regular Expression Syntax and Metacharacters" on page 348 for more information about regular expressions.)

- **Import** - Click this option to import a line-delimited list of addresses from a file. In the **Import Recipient Address File** dialog box, select the file that contains the recipient addresses, and then click **Open**.
- **Delete** - Select the recipient address(es) to delete (hold down the Ctrl key to select multiple items), and then click **Delete**. Click **Yes** to confirm the deletion.

To set recipient active directory group names for a Message Capture Policy

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Message Capture Policy Sets**.
3. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **New Message Capture Policy Set**.
 - On the toolbar, click **New**.
 - Right-click the selected item, and then click **New Message Capture Policy Set**.
4. In the **New Message Capture Policy Set** dialog box, click the **Policies** tab.
5. Click **Add** to open the **New Policy** dialog box.
6. Click the **Recipient** tab.
7. Under the **Recipient Active Directory Group Names** area, you can use the following options:
 - **Add** - Click this option to define recipient active directory group names. In the **Add Recipient Group** dialog box, type the group name (not case sensitive), and then click **OK**.
 - **Import** - Click this option to import a line-delimited list of group names from a file. In the **Import Recipient Group Names File** dialog box, select the file that contains the group names, and then click **Open**.
 - **Delete** - Select the group name(s) to delete (hold down the Ctrl key to select multiple items), and then click **Delete**. Click **Yes** to confirm the deletion.

This page was intentionally inserted without content.



CHAPTER 8

Report Management

Report Management Overview	224
Report Management File Sets Overview	224
Report Management Jobs	225
Add Report Management Jobs	228
Report Management Parsing Engine Overview	253
Report Management Errors	254



Report Management Overview

The PaperVision Enterprise Report Management product is an optional, separately-licensed component that performs COLD/ERM processing on print streams to prepare them for storage in PaperVision Enterprise. By processing the print stream, the need to scan source documents is eliminated. After the information is in the system, you can distribute printed reports and documents as needed.

To define parameters for processing the print stream, you create Report Management Jobs. As the print stream is processed, document index data is extracted, and the content of the print stream is parsed into manageable pieces of data called "Report Management File Sets" that are appended to data groups. Report Management File Sets are specific to each entity and can be imported using the same process for importing data groups or by a configured Report Management Job.

See the following related sections for more information:

- See "Report Management File Sets Overview" below for information about the contents of Report Management File Sets.
- See "Report Management File Sets" on page 127 for tasks you can perform for Report Management Files Sets that are in the system.
- See "Report Management Jobs" on the facing page for tasks you can perform for existing Report Management Jobs.
- See "Add Report Management Jobs" on page 228 to access instructions to complete this task.
- See "Report Management Parsing Engine Overview" on page 253 for information about the process that occurs when Report Management Jobs run.
- See "Report Management Errors" on page 254 for information about errors logged for Report Management Jobs.

Report Management File Sets Overview

As PaperVision Enterprise Report Management processes print streams, they are parsed into manageable pieces of data called Report Management File Sets that are appended to data groups. Report management jobs define parameters for how print streams are processed. (See "Report Management Jobs" on the facing page for more information.)

Report Management File Sets are specific to each entity and can be imported using the same process for importing data groups or by a configured Report Management Job. (See "Import Data Groups" on page 101 and "Report Management Jobs" on the facing page for instructions.) See "Report Management File Sets" on page 127 to access instructions for tasks you can perform on Report Management File Sets after they are imported.

The primary value of Report Management File Sets is the ability to perform a "roll back," which deletes the data it contains. This function is useful to remove Report Management File Sets created by an incorrectly-configured job without affecting the rest of the information in the data group. (See "Roll Back Report Management File Sets" on page 131 for more information about this function.)

Each Report Management File Set contains at least the following files:

- **Data File(s)** - These files contain the output page data. They are named with either a .PVERMDATx extension or a .PVERMCDATx extension when the data in the files set is compressed.
- **Offset File(s)** - These files contain the offset data that is used to calculate where a specific page of data can be located within the corresponding data file. They are named with a .PVERMOFFx extension.
- **Document File** - This file contains the document index values and the file set page numbers for the start and end pages of the document. It is named with a .PVERMDOC extension.
- **Info File** - This file contains the XML document describing the project configuration. It is named with a .PVERMINFO extension.
- **Submit File** - This file contains internal information pertaining to the parsing engine. It is named with a .PVERMSUBMIT extension.
- **Summary File** - This file contains the XML document describing which files were processed into the file set, the date and time the file set was started and finished, the total amount of processing time, and the total number of documents, pages, and bytes. It is named with a .PVERMSUMM extension.

If the Report Management Job includes form overlays, the file set will also include:

- **Overlay Definition File** - This file contains the XML document describing the form overlay configurations and application rules. It is named with the .PVERMOLDEF extension.
- **Overlay Image File(s)** - These files are the actual image files used as blank overlays when rendering a form overlay. They are named with a .PVERMOLx extension.

Report Management Jobs

Report Management Jobs define parameters for processing print streams to create manageable pieces of data called Report Management File Sets that are appended to data groups. See "Report Management Overview" on the previous page for access to information about the contents of Report Management File Sets and the process that occurs when Report Management Jobs run.



NOTE

The following procedures describe tasks you can perform for existing Report Management Jobs. See "Add Report Management Jobs" on page 228 for instructions to create new Report Management Jobs

To view Report Management Jobs

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Projects**.

3. Expand the appropriate project, and then click **Report Management Jobs**.

The right pane shows a list of defined Report Management Jobs and shows for each one the:

- Name
- Status (whether the Report Management Job is active or inactive; inactive jobs display with a red background)
- Input paths to be monitored for files
- Workstation to monitor the specified paths

To import Report Management Jobs



NOTE

Before performing this procedure, make sure that you have a properly-formatted XML file that was created by exporting a Report Management Job. See "To export Report Management Jobs to an XML file" on the facing page for instructions. All of the Report Management Job configuration information is included, except for the input paths that you must configure separately. The XML file also includes the form overlay image files.

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Projects**.
3. Expand the appropriate project, and then click **Report Management Jobs**.
4. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Import**.
 - On the toolbar, click **Import**.
 - Right-click the selected item, and then click **Import**.
5. In the **Import Report Management Job** dialog box, select the XML file that contains the Report Management Job information, and then click **Open**.
6. Click **OK** in the confirmation message.

To refresh the Report Management Jobs list

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Projects**.
3. Expand the appropriate project, and then click **Report Management Jobs**.
4. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Refresh**.
 - On the toolbar, click **Refresh**.
 - Right-click the selected item, and then click **Refresh**.

To delete Report Management Jobs

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Projects**.
3. Expand the appropriate project, and then click **Report Management Jobs**.

4. On the right pane, select the Report Management Job(s) to delete (hold down the Ctrl key to select multiple items).
5. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Delete**.
 - On the toolbar, click **Delete**.
 - Right-click the selected item, and then click **Delete**.
6. Click **Yes** to confirm the deletion.

To export Report Management Jobs to an XML file



NOTE

The exported Report Management Job includes all of the Report Management Job configuration information, except for the input paths. For ease of transport, the XML file also includes the form overlay image files.

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Projects**.
3. Expand the appropriate project, and then click **Report Management Jobs**.
4. On the right pane, select the Report Management Job to export.
5. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Export**.
 - On the toolbar, click **Export**.
 - Right-click the selected item, and then click **Export**.
6. In the **Export Report Management Job** dialog box, select the location where the export file will go.
7. In the **File Name** box, type a name for the export file, and then click **Save**.

To edit properties for Report Management Jobs

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Projects**.
3. Expand the appropriate project, and then click **Report Management Jobs**.
4. On the right pane, select the Report Management Job.
5. Do one of the following:
 - Double-click the selected item.
 - On the **Action** menu, point to **All Tasks**, and then click **Properties**.
 - On the toolbar, click **Properties**.
 - Right-click the selected item, and then click **Properties**.
6. In the **Report Management Job Properties** dialog box, make your changes. (See "Add Report Management Jobs" on the next page for access to option descriptions.)
7. When you are finished modifying the properties, click **Save**.

To deactivate or activate Report Management Jobs

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Projects**.
3. Expand the appropriate project, and then click **Report Management Jobs**.
4. On the right pane, select the Report Management Job.
5. Do one of the following:
 - Double-click the selected item.
 - On the **Action** menu, point to **All Tasks**, and then click **Properties**.
 - On the toolbar, click **Properties**.
 - Right-click the selected item, and then click **Properties**.
6. On the **General** tab, do one of the following:
 - To deactivate the Report Management Job, clear the **Active** check box.
 - To activate the Report Management Job, select the **Active** check box.
7. Click **Save**.

Add Report Management Jobs

Report Management Jobs contain settings that define how print streams are processed. (See "Report Management Jobs" on page 225 for instructions for tasks you can perform for existing Report Management Jobs.) When you create a Report Management Job, you set options on the following tabs:

- **General** - On this tab, you specify the name, input path, default font, data group options, and whether the Report Management Job is active. You can also choose to perform analysis on a sample input file to determine what other configuration options might be helpful.
- **File** - On this tab, you configure the block size, translation type, character replacement, test sequence removal, and file header options.
- **Line** - On this tab, you specify the line delimiter type, fixed-line width, and options for line processing.
- **Page** - On this tab, you configure the page detection method and related page preamble settings.
- **Fields/Breaks** - On this tab, you can view the index fields defined for extraction, specify the maximum number of pages per document, configure the sample process settings, and configure document index fields and breaks.
- **Form Overlays** - On this tab, you can add, edit, remove, and reorder form overlays.

To add Report Management Jobs

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Projects**.
3. Expand the appropriate project, and then click **Report Management Jobs**.

4. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **New Report Management Job**.
 - On the toolbar, click **New**.
 - Right-click the selected item, and then click **New Report Management Job**.
5. In the **New Report Management Job** dialog box, specify the options on each tab.
For information about the options on each tab, see the following:
 - See "General Settings" below for instructions to set options on the **General** tab.
 - See "File Settings" on the next page for instructions to set options on the **File** tab.
 - See "Line Settings" on page 232 for instructions to set options on the **Line** tab.
 - See "Page Settings" on page 233 for instructions to set options on the **Page** tab.
 - See "Fields and Breaks Settings" on page 241 for instructions to set options on the **Fields/Breaks** tab.
 - See "Form Overlay Settings" on page 249 for instructions to set options on the **Form Overlays** tab.
6. When you are finished setting the options on each tab, click **Save**.

General Settings

This content describes how to set the general options for a Report Management Job. On the **General** tab, you specify the name, input path, default font, data group options, and whether the Report Management Job is active. You can also choose to perform analysis on a sample input file to determine what other configuration options might be helpful.

To set general options for a Report Management Job

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Projects**.
3. Expand the appropriate project, and then click **Report Management Jobs**.
4. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **New Report Management Job**.
 - On the toolbar, click **New**.
 - Right-click the selected item, and then click **New Report Management Job**.
5. On the **General** tab, you can set the following options:
 - **Name** - This setting specifies the name of the Report Management Job.
 - **Input Paths** - This area specifies the path(s) that the parsing engine will check for files to process. We recommend that you use a Universal Naming Convention (UNC) path (for example, \\Servername\Sharename). To add a path, click **Add**, and then do one of the following:
 - In the **Path** box, type the input path, and then click **OK**.
 - Click the ellipsis button, select the input path, click **OK**, and then click **OK** again.
 - **Default Font** - This area specifies the font to be used for configuring fields and document breaks. To specify font options, click **Select**, specify font options, and then click **OK**.

- **Max. Data Group Size (MB)** - This setting specifies in megabytes the maximum size allowed for a data group after a file set is appended to it. After a file set is created by the Report Management Job, it looks for a read/write-enabled data group with enough space to append the file set without exceeding this value. If a suitable data group is not found, a new data group is automatically created for the file set.
- **Max. File Set Size (MB)** - This setting specifies in megabytes the maximum size for each file set. This setting specifies the maximum size of each file set. This setting is particularly useful for limiting how much data would be "rolled back" when a configuration mistake is made. This value is considered only after an entire document has been written to a file set so that a single document will not be spread across multiple file sets. This could result in the file set size exceeding this value in some instances.
- **File Set Encryption Key** - This setting specifies the encryption key to be used when the file set is created. If a file set is encrypted, when documents are retrieved from the file set, they are automatically decrypted for viewing.
- **Compress Output Data** - This setting specifies whether page contents are compressed prior to being written to the data file for the file set. Compressing the output increases system overhead during processing, importing data groups, and retrieving documents, but significantly decreases the size of the resulting file set.
- **Import During Processing** - This setting specifies whether a created file set is immediately imported and appended to a data group.
- **Active** - This setting specifies whether the Report Management Job is to be run during automated processing.
- **Analyze File** - This option performs analysis on a portion of a sample input file. To run an analysis, click **Analyze File**. Results appear in the **File Analysis** dialog box and offers clues as to the contents of the file and different settings that might be helpful. For instance, it can recommend to use EBCDIC translation if it suspects that the file is not an ASCII file. Also, line delimiting might be recommended based on the carriage return/line feed count. In addition to these recommendations, a character count is displayed that shows the ASCII decimal value, hexadecimal value, and number of occurrences of each character. This can be useful in determining if certain hidden characters need to be replaced or discarded (such as Null characters).

File Settings

This content describes how to set the file options for a Report Management Job. On the **File** tab, you configure the block size, translation type, character replacement, test sequence removal, and file header options.

To set file options for a Report Management Job

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Projects**.
3. Expand the appropriate project, and then click **Report Management Jobs**.
4. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **New Report Management Job**.
 - On the toolbar, click **New**.

- Right-click the selected item, and then click **New Report Management Job**.
5. On the **File** tab, you can set the following options:
 - **Block Size (KB)** - This setting specifies in kilobytes the size of portions of data called “blocks” that the parser reads from incoming files. This setting lets you fine-tune the size of the block that is imported. Larger block sizes are generally faster because fewer file reading operations are required, but they could bog down a server with little available memory.
 - **Translation** - This setting specifies the translation method used for EBCDIC processing. You can choose one of the following options:
 - ASCII (No Translation)
 - EBCDIC - CP037 US/Canada 3270 Superset
 - EBCDIC - CP500 International Latin 1
 - EBCDIC - Base 3270 ASCII Superset
 - **Character Replacement** - This area lets you configure character replacement options. After a block of data is read, the parsing engine can perform character removal or replacement before any further processing occurs. This is particularly useful for removing hidden characters, such as null characters. See “To configure character replacement options” below for instructions.
 - **Text Sequence Removal (Raw Buffer)** - This area lets you configure options to search for and remove regular expressions. This process begins after any character replacement operations are complete and before any further processing occurs. This option is useful when reports have embedded printer codes that cannot be processed or include mainframe job-related information embedded within files. This process extracts bothersome control sequences that affect page output and display. See “To configure text sequence removal options” on the next page for instructions.
 - **File Preamble Discard** - This setting specifies the type of header information to be stripped prior to processing. You can choose lines, words, or characters.
 - **Quantity to Discard** - This setting specifies the number of items (lines, words, or characters) to be stripped from the beginning of each file prior to processing.
 - **File Preamble Insert Spaces** - This setting specifies how many blank spaces should be inserted at the beginning of each file’s data. This option is useful in instances that require the insertion of spaces so that the remainder of the data lines up properly.

To configure character replacement options

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Projects**.
3. Expand the appropriate project, and then click **Report Management Jobs**.
4. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **New Report Management Job**.
 - On the toolbar, click **New**.
 - Right-click the selected item, and then click **New Report Management Job**.
5. Click the **File** tab.
6. In the **Character Replacement** area, click **Configure**.

7. In the **Character Replacements** dialog box, click **Add**.
8. In the **Character Replacement Definition** dialog box, you can set the following options:
 - **From ASCII** - This setting specifies the ASCII character to be replaced or discarded.
 - **From Decimal** - This setting specifies the decimal number of the character to be replaced or discarded.
 - **From Hex** - This setting specifies the hexadecimal number of the character to be replaced or discarded.
 - **Discard** - This check box, when selected, specifies that the character is to be discarded. When the check box is cleared, the character is to be replaced.
 - **To ASCII** - This setting specifies the ASCII character to replace the specified character.
 - **To Decimal** - This setting specifies the decimal number of the character to replace the specified character.
 - **From Hex** - This setting specifies the hexadecimal number of the character to replace the specified character.
9. Click **OK**.

To configure text sequence removal options

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Projects**.
3. Expand the appropriate project, and then click **Report Management Jobs**.
4. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **New Report Management Job**.
 - On the toolbar, click **New**.
 - Right-click the selected item, and then click **New Report Management Job**.
5. Click the **File** tab.
6. In the **Text Sequence Removal** area, click **Configure**.
7. In the **Text Sequence Removal** dialog box, click **Add**.
8. In the **Regular Expression** box, type the regular expression, and then click **OK**. (See "Regular Expression Syntax and Metacharacters" on page 348 for more information.)

Line Settings

This content describes how to set the line options for a Report Management Job. On the **Line** tab, you specify the line delimiter type, fixed-line width, and options for line processing.

To set line options for a Report Management Job

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Projects**.
3. Expand the appropriate project, and then click **Report Management Jobs**.

4. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **New Report Management Job**.
 - On the toolbar, click **New**.
 - Right-click the selected item, and then click **New Report Management Job**.
5. On the **Line** tab, you can set the following options:
 - **Line Delimiter Type** - This setting specifies the delimiter type used to assemble the processed raw data into lines on a page. The **Analyze File** operation can assist you in determining the correct value to use for this setting. (See "General Settings" on page 229 for instructions.) You can choose one of the following options:
 - **CR/LF** - This value uses the carriage return/line feed combination to delimit lines from each other.
 - **CR Only** - This value uses only the carriage return character to delimit lines from each other.
 - **LF Only** - This value uses only the line feed character to delimit lines from each other.
 - **Null Character** - This value uses the null character to delimit lines from each other.
 - **Fixed Line Width** - This value specifies that each line is a fixed number of characters wide.
 - **Fixed Line Width** - This setting specifies the number of characters in each line when using the **Fixed Line Width** value for the **Line Delimiter Type**.
 - **Line Pre-Processing** - In this area you specify options that are applied to lines of text before they are organized into pages. You can set the following items:
 - **Leading Characters to Remove** - This setting specifies the number of leading characters to remove from each line of text.
 - **Leading Spaces to Insert** - This setting specifies the number of spaces to insert at the beginning of each line of text.
 - **Line Post-Processing** - In this area you specify options that are applied to lines of text after they are organized into pages. You can set the following items:
 - **Leading Characters to Remove** - This setting specifies the number of leading characters to remove from each line of text.
 - **Leading Spaces to Insert** - This setting specifies the number of spaces to insert at the beginning of each line of text.
 - **Maximum Line Width** - This setting specifies the maximum width for lines on the page. You can use this value to truncate the length of each line and remove extraneous data from the ends of lines.

Page Settings

This content describes how to set the page options for a Report Management Job. On the **Page** tab, you configure the page detection method and related page preamble settings.

To set page options for a Report Management Job

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.

2. Expand the appropriate entity, and then expand **Projects**.
3. Expand the appropriate project, and then click **Report Management Jobs**.
4. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **New Report Management Job**.
 - On the toolbar, click **New**.
 - Right-click the selected item, and then click **New Report Management Job**.
5. On the **Page** tab, you can set the following options:
 - **Page Detection** - This area lets you configure methods used to organize lines into pages of text. You can choose one of the following options:
 - **Max Lines per Page** - This page detection method places the number of lines specified in the **Max. Lines per Page** box on the page. After the maximum value is reached, a new page is created.
 - **Form-Feed Character** - This page detection method is by far the simplest and fastest detection method. Many systems insert a form feed character (decimal 12) where new pages should begin. Use of this detection method will cause the system to identify the form feeds and break the pages appropriately.
 - **Text Sequence(s)** - This page detection method provides for the definition of one or more text sequences which, once located, designate a specified distance from the top or bottom of a page. You can add, edit, or remove individual sequences. (See "Configure Text Sequences" on page 236 for more information and configuration instructions.)
 - **Custom Control Codes** - This page detection method provides for the identification of a single character or a string of characters that are located within a defined column boundary. This method can be used to separate pages and format output, for example, it can insert blank lines and place text on specific lines. You can add, edit, or remove individual custom codes. (See "Configure Custom Control Codes" on page 237 for more information and configuration instructions.)
 - **ASA/ANSI with Channel Commands** - This page detection method provides a set of 16 codes used for line printers. (See "Configure ASA/ANSI with Channel Commands" on page 238 for more information and configuration instructions.)
 - **AS400 Spool** - This page detection method provides a means of interpreting standard control codes that appear in AS400 spool files. (See "Configure AS400 Spool" on page 240 for more information and configuration instructions.)
 - **Page Preamble Discard Type** - This setting specifies to have lines, words, or characters stripped from the beginning of each page. This process occurs after the page has been assembled from lines and before any further processing occurs. This option is useful when the file has been pre-processed to insert markers to split pages, but those markers shouldn't appear in the resulting output.
 - **Quantity to Discard** - This setting specifies the number of items (lines, words, or characters) to be stripped from the beginning of each page.
 - **Expand to Max Lines** - This setting specifies whether to append blank lines to the end of pages until they meet the value specified in the **Max Lines per Page** setting.

- **Max Lines per Page** - This setting specifies the maximum number of lines per page. This value is used by the **Max Lines per Page** page detection method and the **Expand to Max Lines** setting.
- **Text Sequence Removal** - This area lets you configure options to search for and remove or replace textual values or regular expressions. You define text sequences that designate a specified distance from the top or bottom of a page. This process begins after the page of data is assembled. This option is useful for re-purposing confidential data for use by third parties. You can add, edit, or remove individual text sequences. (See "To configure text sequence removal options" below for instructions.)
- **Page Preamble Insertion Type** - This setting specifies to have blanks lines or characters inserted at the beginning of each page.
- **Quantity to Insert** - This setting specifies the number of items (lines or characters) to be inserted at the beginning of each page.
- **Delete Blank Pages** - This setting specifies whether to delete pages containing only empty lines from the output.

To configure text sequence removal options

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Projects**.
3. Expand the appropriate project, and then click **Report Management Jobs**.
4. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **New Report Management Job**.
 - On the toolbar, click **New**.
 - Right-click the selected item, and then click **New Report Management Job**.
5. Click the **Page** tab.
6. In the **Text Sequence Removal** area, click **Configure**.
7. In the **Text Sequence Removal** dialog box, click **Add**.
8. In the **Text Sequence Removal Definition** dialog box, you can set the following options:
 - **Sequence** - This setting specifies the text or regular expression to find. (See "Regular Expression Syntax and Metacharacters" on page 348 for more information.)
 - **Regular Expression** - This setting specifies whether the value in the **Sequence** box is handled as a regular expression (when selected) or searched for as a text value (when cleared).
 - **Min. Column** - This setting specifies the minimum column that the text sequence must fall within.
 - **Max. Column** - This setting specifies the maximum column that the text sequence must fall within.
 - **Min. Line** - This setting specifies the minimum line that the text sequence must fall within.
 - **Max. Line** - This setting specifies the maximum line that the text sequence must fall within.
 - **Disposition** - This setting specifies what to do with the text sequence after it is located.
9. Click **OK** to save the defined text sequence.

Page Detection Methods

For Report Management Jobs, there are several page detection methods you can configure to detect and organize lines into pages.

- **Max Lines per Page** - This page detection method places the number of lines specified in the **Max. Lines per Page** box on the page. After the maximum value is reached, a new page is created. (See "Page Settings" on page 233 for configuration instructions.)
- **Form-Feed Character** - This page detection method is by far the simplest and fastest detection method. Many systems insert a form feed character (decimal 12) where new pages should begin. Use of this detection method will cause the system to identify the form feeds and break the pages appropriately. (See "Page Settings" on page 233 for configuration instructions.)
- **Text Sequence(s)** - This method uses the specified text or regular expression to detect pages. (See "Configure Text Sequences" below for more information and configuration instructions.)
- **Custom Control Codes** - This method identifies a single character or a string of characters within a defined column boundary to detect pages. (See "Configure Custom Control Codes" on the facing page for more information and configuration instructions.)
- **ASA/ANSI with Channel Commands** - This page detection method provides a set of 16 codes used for line printers. (See "Configure ASA/ANSI with Channel Commands" on page 238 for more information and configuration instructions.)
- **AS400 Spool** - This page detection method provides a means of interpreting standard control codes that appear in AS400 spool files. (See "Configure AS400 Spool" on page 240 for more information and configuration instructions.)

Configure Text Sequences

The **Text Sequence(s)** method provides for the definition of one or more text sequences which, once located, designate a specified distance from the top or bottom of a page. You can add, edit, or remove individual sequences.

To configure text sequences

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Projects**.
3. Expand the appropriate project, and then click **Report Management Jobs**.
4. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **New Report Management Job**.
 - On the toolbar, click **New**.
 - Right-click the selected item, and then click **New Report Management Job**.
5. Click the **Page** tab.
6. From the **Detection Method** list, select **Text Sequence(s)**.
7. In the **Page Detection** area, click **Configure**.
8. In the **Text Sequence Page Detection** dialog box, click **Add**.

9. In the **Text Sequence Definition** dialog box, you can set the following options:
 - **Sequence** - This setting specifies the text or regular expression to find. (See "Regular Expression Syntax and Metacharacters" on page 348 for more information.)
 - **Regular Expression** - This setting specifies whether the value in the **Sequence** box is handled as a regular expression (when selected) or searched for as text value (when cleared).
 - **Min. Column** - This setting specifies the minimum column that the text sequence must fall within.
 - **Max. Column** - This setting specifies the maximum column that the text sequence must fall within.
 - **Page Effect** - This area specifies the location for the page beginning or ending after the text sequence is located in the specified columns. You can select one of the following options:
 - **Page begins** - This setting specifies the number of lines above the found text sequence to begin the page. A value of zero specifies that the located text sequence is the top line of the page.
 - **Page ends** - This setting specifies the number of lines below the found text sequence to end the page. A value of zero specifies that the located text sequence is the bottom line of the page.
 - **Disposition** - This setting specifies what to do with the text sequence after it is located.
10. Click **OK** to save the defined text sequence.

Configure Custom Control Codes

The **Custom Control Codes** method provides for the identification of a single character or a string of characters that are located within a defined column boundary. This method can be used to separate pages and format output, for example, it can insert blank lines and place text on specific lines. You can add, edit, or remove individual custom codes.

To configure custom control codes

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Projects**.
3. Expand the appropriate project, and then click **Report Management Jobs**.
4. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **New Report Management Job**.
 - On the toolbar, click **New**.
 - Right-click the selected item, and then click **New Report Management Job**.
5. Click the **Page** tab.
6. From the **Detection Method** list, select **Custom Control Codes**.
7. In the **Page Detection** area, click **Configure**.
8. In the **Control Code Settings** area, you can set the following options:
 - **Start Column** - This setting specifies the starting column position for each line that will be evaluated for custom codes.

- **Column Width** - This setting specifies the width from the start column that will be used to evaluate custom codes. For example, if the start column is 5 and the column width is 5, then codes that fall within columns 5, 6, 7, 8 and 9 will be evaluated.
 - **Vertical Space on Undefined Codes** - This setting specifies whether a vertical space (carriage return or line feed) is inserted when an undefined code is found.
 - **Strip Codes** - This setting, when selected, specifies that the columns in the **Start Column** and **Column Width** settings are removed from the output.
9. In the **Custom Codes** area, click **Add**.
10. In the **Custom Code Definition** dialog box, you can set the following options:
- **ASCII** - This setting specifies the ASCII character(s) of the custom code.
 - **Decimal** - This setting specifies the decimal value(s) of the character(s) of the custom code.
 - **Hex** - This setting specifies the hexadecimal value(s) of the character(s) of the custom code.
 - **Action** - This setting specifies what to do when the code is found. You can choose one of the following options:
 - **Ignore/No Action** - This setting specifies that the code is defined, but no action is taken when it is found.
 - **Move to Line** - This setting specifies that the system moves to the line number specified by the **Value** setting, and then outputs the remainder of the input line. If the specified line number is below the current line of the page, it moves to the specified line of the current page. If the specified line number is above the current line of the page, a new page is created and then it moves to the specified line of the new page to output.
 - **Vertical Space** - This setting specifies that the number of vertical spaces (carriage return or line feed) specified by the **Value** property is inserted before writing out the remainder of the input line
 - **End Page, Then Move to Line** - This setting specifies that the remainder of the input line is immediately written to the current page. Then, a new page is created, and the system moves to the line number specified by the **Value** property.
 - **Value** - This setting specifies the number of items used by the value in the **Action** box.
11. Click **OK** to save the defined custom code.

Configure ASA/ANSI with Channel Commands

The **ASA/ANSI with Channel Commands** method provides a set of 16 codes used for line printers. Each code dictates the carriage control (line movement) prior to writing the remainder of the line to output. When the remainder of the line is written, the carriage control remains on the current output line and does not automatically go to a new output line. The first four codes are static and described below:

- **+** (plus sign) - This code does not move the carriage control. It outputs the remainder of the input line, so it effectively combines the current line with the previous line.
- **(blank space)** - This code inserts a single vertical space (carriage return or line feed), and then outputs the remainder of the line.
- **0** (zero) - This code inserts two vertical spaces (carriage returns or line feeds), and then outputs the remainder of the line.

- - (minus sign) - This code inserts three vertical spaces (carriage returns or line feeds) and then outputs the remainder of the line.

The remaining twelve codes are dynamic and are known as "channels." You can define the action taken for each of the remaining twelve codes. Channel 1 is the most common, and by standards is generally used to indicate "top of form."

To configure ASA/ANSI with channel commands

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Projects**.
3. Expand the appropriate project, and then click **Report Management Jobs**.
4. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **New Report Management Job**.
 - On the toolbar, click **New**.
 - Right-click the selected item, and then click **New Report Management Job**.
5. Click the **Page** tab.
6. From the **Detection Method** list, select **ASA/ANSI with Channel Commands**.
7. In the **Page Detection** area, click **Configure**.
8. In the **Control Code Settings** area, you can set the following options:
 - **Start Column** - This setting specifies the starting column position for each line that will be evaluated for channel codes. The ASA/ANSI reports generally use a start column of 1.
 - **Column Width** - This setting specifies the width from the start column that will be used to evaluate channel codes. For example, if the start column is 5 and the column width is 5, then channel codes that fall within columns 5, 6, 7, 8 and 9 will be evaluated. The ASA/ANSI reports generally use a column width of 1.
 - **Strip Codes** - This setting, when selected, specifies that the columns in the **Start Column** and **Column Width** settings are removed from the output.
9. In the **Skip To Channel Codes** area, for each listed channel, you can set the following options:
 - **Action** - This setting specifies what to do when the channel code is found. You can choose one of the following options:
 - **Ignore/No Action** - This setting specifies that the channel code is ignored when it is found. No action is taken and the remainder is tagged onto the previous line.
 - **Move to Line** - This setting specifies that the system moves to the line number specified by the **Action Value** setting, and then outputs the remainder of the input line. If the specified line number is below the current line of the page, it moves to the specified line of the current page. If the specified line number is above the current line of the page, a new page is created and then it moves to the specified line of the new page to output.
 - **Vertical Space** - This setting specifies that the number of vertical spaces (carriage return or line feed) specified by the **Action Value** property is inserted before writing out the remainder of the input line
 - **Action Value** - This setting specifies the number of items used by the value in the **Action** box.

10. Click **OK** to save the defined channel codes.

Configure AS400 Spool

The **AS400 Spool** method provides a means of interpreting standard control codes that appear in AS400 spool files. The common theme behind this type of control scenario is that a three-digit number, a one-digit number, or nothing is located within the code columns. The command is carried out, inserting the appropriate number of vertical spaces (carriage returns or line feeds), and then the remainder of the input line is appended. When the remainder of the line is written, the carriage control remains on the current output line and does not automatically go to a new output line. The spool codes are described below:

- (blank space) - This code inserts a single vertical space (carriage return or line feed), and then outputs the remainder of the input line.
- One-digit number - This code inserts the specified number of vertical spaces (carriage returns or line feeds), and then outputs the remainder of the line.
- Three -digit number - This code advances to the specified line number on the page, and then outputs the remainder of the input line. If the specified line number is less than the current line number of the current page, a new page is created and the system advances to the specified line number before outputting the remainder of the input line.

To configure AS400 spool codes

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Projects**.
3. Expand the appropriate project, and then click **Report Management Jobs**.
4. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **New Report Management Job**.
 - On the toolbar, click **New**.
 - Right-click the selected item, and then click **New Report Management Job**.
5. Click the **Page** tab.
6. From the **Detection Method** list, select **AS400 Spool**.
7. In the **Page Detection** area, click **Configure**.
8. In the **AS400 Spool Page Detection** dialog box, you can set the following options:
 - **Start Column** - This setting specifies the starting column position for each line that will be evaluated for spool codes. AS400 spool files generally use a start column of 1.
 - **Column Width** - This setting specifies the width from the start column that will be used to evaluate spool codes. For example, if the start column is 5 and the column width is 5, then spool codes that fall within columns 5, 6, 7, 8 and 9 will be evaluated. AS400 spool files generally use a column width of 4.
 - **Strip Codes** - This setting, when selected, specifies that the columns in the **Start Column** and **Column Width** settings are removed from the output.
9. Click **OK** to save the defined AS400 spool codes.

Fields and Breaks Settings

This content describes how to set the fields and breaks options for a Report Management Job. On the **Fields/Breaks** tab, you can view the index fields defined for extraction, specify the maximum number of pages per document, configure the sample process settings, and configure document index fields and breaks.

To set fields/breaks options for a Report Management Job

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Projects**.
3. Expand the appropriate project, and then click **Report Management Jobs**.
4. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **New Report Management Job**.
 - On the toolbar, click **New**.
 - Right-click the selected item, and then click **New Report Management Job**.
5. On the **Fields/Breaks** tab, you can set the following options:
 - **Project Index Fields** - This area displays the project index fields that are defined for extraction.
 - **Maximum Pages per Document** - This setting specifies that a new document will automatically be started when the document page count reaches this number. A value of zero disables this feature.
 - **Output Path** - This setting specifies the temporary location for file sets that are created when you click the **Configure Fields/Breaks** or **Text Execution** button. Clicking either button causes the parsing engine to run as it will when automated. The created file sets are removed automatically when you close the window that opens after the files are processed. We recommend that you use a Universal Naming Convention (UNC) path (for example, \\Server-name\Sharename). To add a path, do one of the following:
 - In the **Output Path** box, type the temporary output directory.
 - Click the ellipsis button, select the temporary output directory, and then click **OK**.
 - **Blocks to Run** - This setting specifies the number of blocks of data that will process when you click the **Configure Fields/Breaks** or **Text Execution** button. (See "To set file options for a Report Management Job" on page 230 to specify the block size.) This option lets you limit how much data is run through the parser prior to displaying the results. This is useful when configuring a job for large reports, as it is seldom necessary to parse an entire report to configure the job. Setting a value of zero causes the parser to process all of the data in the file.
 - **Configure Fields/Breaks** - Clicking this button parses the specified blocks of data, and then opens the **Configure Fields/Breaks** window where you can define regions, anchors, and fields. (See "Configure Fields and Breaks" on the next page for more information.)
 - **Test Execution** - Clicking this button runs a "real-world" test of the job configuration, and then opens the **Test Execution Results** window where you can see the resulting output, including index values. (See "Test Execution" on page 247 for more information.)

Configure Fields and Breaks

After you configure the settings on the **Fields/Breaks** tab, you can work with sample documents to configure how index fields are extracted and documents breaks are inserted. From the **Fields/Breaks** tab, when you click the **Configure Fields/Breaks** button, the system parses the sample document(s) into pages. These pages are then displayed in the **Configure Fields/Breaks** window where you can set configuration options. To configure the extraction of document indexes, it is beneficial to understand what regions and anchors are, and how they are used to extract index values. See "Document Indexing Terms and Concepts" on page 246 for more information. See "Report Management Parsing Engine Overview" on page 253 to understand how the system processes index information.



NOTE










Before you perform the following procedures, ensure that all other items on the **Fields/Breaks** tab are configured. See "Fields and Breaks Settings" on the previous page for instructions.

To access fields and breaks configuration options

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Projects**.
3. Expand the appropriate project, and then click **Report Management Jobs**.
4. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **New Report Management Job**.
 - On the toolbar, click **New**.
 - Right-click the selected item, and then click **New Report Management Job**.
5. Click the **Fields/Breaks** tab, and then click **Configure Fields/Breaks**.

The sample document is processed and parsed into pages. Then, these pages appear in the **Configure Fields/Breaks** window, where you can configure fields and breaks using the options described in the following table.

Toolbar Button	Keyboard Shortcut	Menu > Command	Function
	Home	Navigation > First Page	Displays the first page of the processed data
	Page Up	Navigation > Previous Page	Displays the previous page of the processed data
	F3	Navigation > Find Page	Locates a specific page number of the processed data
	Page Down	Navigation > Next Page	Displays the next page of the processed data
	End	Navigation > Last Page	Displays the last page of the processed data

Toolbar Button	Keyboard Shortcut	Menu > Command	Function
	A	View > Show All	Displays all regions, anchors and fields
	C	View > Show Region Components	Displays all components (anchor, ranges, and fields) for the currently selected region
	B	View > Show Document Breaks	Displays all break regions and document break fields
	E	View > Enable/Disable Enlarged Frames	Increases the size of the frame around displayed items so it is easier to select with the mouse
	R	Items > New Region	Starts the mode to draw a new region
	D	Items > New Detail Region	Starts the mode to draw a new detail region
	F	Items > New Field	Starts the mode to draw a new field in the currently selected region
	P	Items > Properties	Displays the properties for the currently selected item
	Delete	Items > Delete	Deletes the currently selected region or field
N/A	Esc	Navigation > Close	Closes the Configure Fields/Breaks window

To configure regions

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Projects**.
3. Expand the appropriate project, and then click **Report Management Jobs**.
4. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **New Report Management Job**.
 - On the toolbar, click **New**.
 - Right-click the selected item, and then click **New Report Management Job**.
5. Click the **Fields/Breaks** tab, and then click **Configure Fields/Breaks**.
The sample file is processed, and then the **Configure/ Fields/Breaks** window appears.
6. To draw a region, do one of the following:
 - On the **Items** menu, click **New Region** or **New Detail Region**.
 - On the toolbar, click **New Region** or **New Detail Region**.

7. Position the pointer where you want to draw the region, and then click and drag the pointer to draw a border around the area where you want the index value extracted.

The **Region Properties** dialog box appears.

8. On the **General** tab, you can set the following options:
 - **Region Name** - This setting specifies a name for the region that is used only for your reference.
 - **Detail Region** - This setting specifies whether the region is a detail region. Detail regions are repeatedly located in the same area on a page for extracting detail data, whereas non-detail regions are located only once on a page.
 - **Break Documents** - This setting, when selected, specifies that a document break is placed when the defined region is found on the page. You can choose one of the following options to specify the position of document breaks:
 - **Current document starts x pages prior to current page** - The setting specifies that the document break is inserted the number of specified pages before the current page. To place the break on the current page, set the page value to zero.
 - **Next document starts x pages after current page** - The setting specifies that the document break is inserted the number of specified pages after the current page. To place the break on the current page, set the page value to zero.
 - **Region Dimensions** - This area specifies the height and width of the region. The **Height** box specifies the region height in lines. The **Width** box specifies the region width in columns. You can specify region dimensions using these values or by moving the region boundaries with the mouse.



N O T E

Regions can fall outside the boundaries of some pages.

- **Region Offset from Anchor** - This area specifies the offset distance from the top left corner of the anchor from which the top left corner of the region is created after an anchor is located. The **Top** box specifies the distance in lines. The **Left** box specifies the distance in columns.
9. To set anchor properties, click the **Anchor** tab. (See "Anchors" on page 247 for more information about the types of anchors and how region boundaries are calculated using anchors.)
 10. From the **Anchor Type** list, select one of the following values:
 - **Fixed Anchor** - This setting specifies that the anchor remains in a fixed location from the top left corner of the page. In the **Fixed Anchor Page Position** area, the values specify the anchor location from the top left corner of the page. The **Top** box specifies the distance in lines. The **Left** box specifies the distance in columns. You can specify the anchor position using these values or the mouse.
 - **Floating Anchor** - This setting specifies that the anchor is not fixed. Floating anchors are located by searching for a sequence of data (that you define) within the page.
 11. If you selected **Floating Anchor** in the previous step, you can set the following options:
 - **Floating Anchor Location Sequence** - This area specifies the text value that the system uses to search for and locate the anchor.

- **Case Sensitive** - This setting specifies whether the text value is case sensitive (when selected) or not (when cleared).
- **Regular Expression** - This setting specifies whether the text value is a regular expression (when selected) or a text value (when cleared). (See "Regular Expression Syntax and Metacharacters" on page 348 for more information.)
- **Floating Anchor Sequence Range** - This area specifies the area in which the anchor must be located. The **Left** box specifies the distance in columns. The **Width** box specifies the width in columns. The **Top** box specifies the distance in lines. The **Height** box specifies the height in lines. You can specify the range dimensions using these values or the mouse.
- **Validator Sequence** - This area specifies the text value that the system uses to search for and validate the anchor on a page. After the system locates an anchor, it attempts to verify that the specified validator sequence can be located.
 - **Case Sensitive** - This setting specifies whether the text value is case sensitive (when selected) or not (when cleared).
 - **Regular Expression** - This setting specifies whether the text value is a regular expression (when selected) or a text value (when cleared). (See "Regular Expression Syntax and Metacharacters" on page 348 for more information.)
- **Validator Sequence Range** - This area specifies the area in which the anchor must be located. The **Left** box specifies the distance in columns. The **Width** box specifies the width in columns. The **Top** box specifies the distance in lines. The **Height** box specifies the height in lines. You can specify the range dimensions using these values or the mouse.

To configure fields



NOTE

Before you can configure fields you must first define regions. (See "To configure regions" on page 243 for instructions.)

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Projects**.
3. Expand the appropriate project, and then click **Report Management Jobs**.
4. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **New Report Management Job**.
 - On the toolbar, click **New**.
 - Right-click the selected item, and then click **New Report Management Job**.
5. Click the **Fields/Breaks** tab, and then click **Configure Fields/Breaks**.
The sample file is processed, and then the **Configure/ Fields/Breaks** window appears.
6. On the left pane, in the **Regions** folder, click the region in which you want to configure a field
7. Do one of the following:
 - On the **Items** menu, click **New Field**.
 - On the toolbar, click **New Field**.

8. Position the pointer, and then click and drag the pointer to draw a border around the area where you want to configure a field.
9. The **Field Properties** dialog box appears, where you can set the following options:
 - **Field Type** - This setting specifies the type of field. You can choose one of the following options:
 - **Index Field and Document Break** - The setting saves the data within the field for document retrieval and when the field data changes, automatically marks a new document.
 - **Index Field Only** - The setting saves the data within the field for document retrieval.
 - **Document Break Only** - The setting checks for changing values and, when the values change, automatically marks a new document.
 - **Field Name** - For index fields, this setting corresponds to the name of the index field that will be populated with the located values.
 - **Break Offset** - For document break fields, this setting specifies the number of pages after the current page that will be appended into the current document before a new document is started. A value of zero indicates that the current page is the last page of the document.
 - **Field Validation Regular Expression** - This area specifies the regular expression used to validate field data. (See "Regular Expression Syntax and Metacharacters" on page 348 for more information.) After field data is extracted, it is compared against this validation sequence to verify that the located value is valid.
 - **Case Sensitive** - This setting specifies whether the regular expression is case sensitive (when selected) or not (when cleared).
 - **Field Location Relative to Region** - This area specifies the left, top, width, and height of the column/line range from which the field value is extracted. The **Left** box specifies the distance in columns. The **Width** box specifies the width in columns. The **Top** box specifies the distance in lines. The **Height** box specifies the height in lines. You can specify the range dimensions using these values or the mouse. If a field is located on multiple lines, the lines are combined with spaces between their values.

Document Indexing Terms and Concepts

The index value extraction capabilities for Report Management Jobs are extensive. To configure the extraction of document indexes, it is beneficial to understand what regions and anchors are, and how they are used to extract index values.

Regions

Regions are areas on a page from which one or many index values are extracted. Regions are either normal regions or detail regions. Each region contains one anchor and zero to many index values.

Normal Regions

Normal regions are used to locate index values that are extracted once within a document (for example, invoice number, date, and customer name) and are located once on a page. After the normal region is located (by its anchor), index values are extracted and the system continues processing any other defined regions. It is common for normal regions to use either fixed or floating anchors.

Detail Regions

Detail regions are used to extract detail information from a document (for example, part numbers from the detail listing of an invoice). After the detail region is located (by its anchor), index values are extracted. The system then repeats the process until it can no longer locate the anchor on the page. Detail regions generally use floating anchors.



NOTE

If a detail region is configured for a job, full-text data will not be imported into the retrieval system since detail field extraction creates "duplicate" documents (multiple document entries pointing to the same set of pages). Duplicate document full-text indexing results in the document being indexed as many times as there are duplicate entries. Generally, the use of detail regions and fields negates the need to perform full-text searches on the documents as the pertinent information has already been extracted.

Anchors

Anchors are used to identify regions on a page. Anchors can either be fixed or floating. After an anchor is located, the region boundaries are determined by the offset from the anchor in columns and rows.

Fixed Anchors

Fixed anchors are always located in the same position on the page, as distanced from the top left corner.

Floating Anchors

Floating anchors are located by searching for a sequence of data within the page. The anchor is placed wherever the sequence is located, the region is identified, and index values are extracted. The system then repeats this process until the sequence is no longer found.

Floating anchors can be located only within their **Floating Anchor Sequence Range**, which is an area of the page in which the sequence search is to be performed.

Floating anchors can also have a **Validator Sequence**. After a floating anchor is located, the system checks to see if the validator sequence can be located within the specified **Validator Sequence Range**. If not, the anchor is discarded. Validator sequences allow a secondary check to occur when the anchor is located.

Fields

Fields are used to extract document index fields or detail data from regions. Field locations are always fixed within their region (relative to the top left corner of the region).

Test Execution














From the **Fields/Breaks** tab, you can click the **Text Execution** button to run a real-world test of the Report Management Job to ensure that it is configured correctly. The results of the test (including document index values), are displayed in the **Text Execution Results** window for your evaluation. Only the documents (up to 20,000) from the first file set are displayed.

You can navigate through the documents and pages by clicking the appropriate toolbar buttons, selecting the corresponding menu items, or using keyboard shortcuts. You can also select specific documents by double-clicking the document in the list.

To run a test and access results

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Projects**.
3. Expand the appropriate project, and then click **Report Management Jobs**.
4. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **New Report Management Job**.
 - On the toolbar, click **New**.
 - Right-click the selected item, and then click **New Report Management Job**.
5. Click the **Fields/Breaks** tab, and then click **Test Execution**.

The sample document is processed and parsed into pages. Then, these pages appear in the **Text Execution Results** window, where you can evaluate the results using the options described in the following table.

Toolbar Button	Keyboard Shortcut	Function
	Home	Displays the first page of the current document
	Page Up	Displays the previous page of the current document
	F3	Locates a specific page number of the current document
	Page Down	Displays the next page of the current document
	End	Displays the last page of the current document
	Ctrl + Home	Displays the first page of the first document
	Ctrl + Page Up	Displays the first page of the previous document
	Ctrl + Page Down	Displays the first page of the next document
	Ctrl + End	Displays the first page of the last document
	O	Shows (or hides) the overlay for the current page
	W	Scales the overlay image to the width of the screen
	H	Scales the overlay image to the height of the screen
	Space	Scales the overlay image to fit on the screen

Form Overlay Settings

This content describes how to set the form overlay options for a Report Management Job. On the **Form Overlays** tab, you can add, edit, remove, and reorder form overlays. When you use form overlays, the parsed page text is placed onto a blank form that creates an image that reproduces the original printed page. An unlimited number of overlay forms are supported per Report Management Job. Each form overlay has a set of rules that are applied to it, and for a form to be selected for a page, all of the rules must be met. When a page of a document is retrieved, all of the rules pertaining to each form overlay are evaluated (in the order that they are listed), until a form overlay is identified that has the rules that are met by that page.



T I P

When configuring jobs that contain a large number of overlays, list the most commonly used forms first, as it increases system responsiveness.

To configure form overlays for a Report Management Job

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Projects**.
3. Expand the appropriate project, and then click **Report Management Jobs**.
4. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **New Report Management Job**.
 - On the toolbar, click **New**.
 - Right-click the selected item, and then click **New Report Management Job**.
5. Click the **Form Overlays** tab, and then click **Add**.
6. In the **New Overlay** dialog box, you can set the following options:
 - **Overlay Name** - This setting specifies the name of the overlay file.
 - **Page Range** - This setting specifies the range of pages to which the overlay form can be applied.
 - **Pages from Range to Include** - This area specifies the pages to which the form can be applied. You can choose **Even Pages**, **Odd Pages**, or **Both Even and Odd Pages**.
 - **Page Content Criteria Regular Expression** - This setting, when specified, causes the system to evaluate whether this regular expression can be located within the contents of the text on the page. (See "Regular Expression Syntax and Metacharacters" on page 348 for more information.)
 - **Case Sensitive** - This setting specifies whether the regular expression is case sensitive (when selected) or not (when cleared).
 - **Index Value Criteria Regular Expression** - This setting, when specified, causes the system to evaluate whether this regular expression can be located within the contents of the specified index field value. (See "Regular Expression Syntax and Metacharacters" on page 348 for more information.)
 - **Case Sensitive** - This setting specifies whether the regular expression is case sensitive (when selected) or not (when cleared).

- **Overlay Image File** - This setting specifies the overlay form file over which the textual content of the page is placed. TIF, JPG, GIF, and PNG image file types are supported. To add a file, do one of the following:
 - In the box, type the path to the overlay image file.
 - Click the ellipsis button, select the path to the overlay image file, and then click **Open**.
- **Setup Overlay** - Clicking this button opens the **Setup Overlay** window where you can configure the rendering of the form overlay (See "Setup Overlay" below for more information.)

Setup Overlay



After you configure the settings for a form overlay, you can work with an overlay image file to view how the output will look. Although you can explicitly set all of the values to generate a correctly-aligned form overlay, working with a sample file lets you graphically modify those settings, and provides immediate feedback about how your changes affect the output.











In the **Setup Overlay** window you can:

- Navigate through the documents and pages by clicking the appropriate toolbar buttons
- Select specific documents by double-clicking the document in the list
- Move the position of the overlay text on the image
- Adjust the text-line height
- Resize the width and height of the blank form
- Set overlay text display properties
- Modify the overlay form
- Revert to the original form




To access setup overlay options

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Projects**.
3. Expand the appropriate project, and then click **Report Management Jobs**.
4. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **New Report Management Job**.
 - On the toolbar, click **New**.
 - Right-click the selected item, and then click **New Report Management Job**.
5. Click the **Form Overlays** tab, and then click **Add**.
6. In the **New Overlay** dialog box, click **Setup Overlay** to open the **Setup Overlay** window where you can use the functions described in the following tables.

Toolbar Button	Keyboard Shortcut	Function
	Home	Displays the first page of the current document
	Page Up	Displays the previous page of the current document

Toolbar Button	Keyboard Shortcut	Function
	F3	Locates a specific page number of the current document
	Page Down	Displays the next page of the current document
	End	Displays the last page of the current document
	Ctrl + Home	Displays the first page of the first document
	Ctrl + Page Up	Displays the first page of the previous document
	Ctrl + Page Down	Displays the first page of the next document
	Ctrl + End	Displays the first page of the last document
	T	Displays the Overlay Text Display Properties dialog box. See "To set overlay text display properties" below for more information.
	F	Displays the Overlay Form Modification dialog box. See "To modify the overlay form" on the next page for more information.
	R	Reverts the displayed form back to the original form (as it was when you first clicked the Setup Overlay button)

In addition to the toolbar buttons, you can use the tools described in the following table. To use these tools, position the pointer on the tool. When the pointer changes to a hand, click and drag the tool to make adjustments.

Tool	Location	Function
 Text Alignment	On the top left corner of the text	Adjusts the position of the overlay text on the image (alters the text left and top values)
 Line Height Adjustment	On the right of the Text Alignment tool	Adjusts the text line height as you increase or decrease the distance between the two lines
 Width and Height Adjustment	On the lower and right edges of the image	Adjusts the width and height of the form as you drag the blue lines

To set overlay text display properties

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Projects**.

3. Expand the appropriate project, and then click **Report Management Jobs**.
4. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **New Report Management Job**.
 - On the toolbar, click **New**.
 - Right-click the selected item, and then click **New Report Management Job**.
5. Click the **Form Overlays** tab, and then click **Add**.
6. In the **New Overlay** dialog box, click **Setup Overlay**.
7. On the toolbar, click **Overlay Text Properties**.
8. In the **Overlay Display Properties** dialog box, you can set the following options:
 - **Overlay Text Font** - This area specifies the font used to render the text on the blank overlay form. Click **Select** to open the **Font** dialog box where you can set font options.
 - **Overlay Text Position** - This area specifies the location where the overlay text is rendered onto the blank form and the height of each line of text (in pixels).

To modify the overlay form

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Projects**.
3. Expand the appropriate project, and then click **Report Management Jobs**.
4. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **New Report Management Job**.
 - On the toolbar, click **New**.
 - Right-click the selected item, and then click **New Report Management Job**.
5. Click the **Form Overlays** tab, and then click **Add**.
6. In the **New Overlay** dialog box, click **Setup Overlay**.
7. On the toolbar, click **Overlay Form Modification**.
8. In the **Overlay Form Modification** dialog box, you can set the following options:
 - **Form Image Resizing** - This area specifies the dimensions of the blank form image. You can modify the **Width** and **Height** properties, and specify whether to **Maintain Aspect Ratio** by selecting or clearing this check box.
 - **Overlay Image Cropping** - This area specifies the number of pixels to remove from each edge of the blank form image.
 - **Overlay Image Add Border** - This area specifies the number of pixels to add to each edge of the blank form image.

Report Management Parsing Engine Overview

The Report Management parsing engine processes information as outlined in the following procedure.



NOTE

See "Add Report Management Jobs" on page 228 to access configuration instructions for the operations referenced in the following procedure.

1. Gets a block of data to parse.
2. If necessary, converts EBCDIC to ASCII.
3. Performs any defined character replacement operations.
4. Performs any defined text sequence removal (raw buffer) operations.
5. If this is the first block of a file, performs any file preamble discard operations.
6. If this is the first block of a file, performs any file preamble insert spaces operations.
7. Using the specified line delimiter type, parses the incoming block of data into an array of lines (these are the same lines as lines on a page).
8. Performs any line pre-processing operations.
9. Using the defined page detection method, a page is assembled from the lines. With the assembled page it does the following:
 1. Performs any line post-processing operations.
 2. Performs any page preamble discard operations.
 3. Performs any page preamble Insert operations.
 4. Performs any text sequence removal operations.
 5. Performs any page length adjustment, such as expand to max lines.
 6. Document index values are extracted from the page.
 7. Document break rules are evaluated. After a document break is identified (using ANY of the configured methods), the new document is assembled and no additional document break rules are evaluated.
 8. Page is written to the output file set.
10. Repeats step 9 for the lines that remain in the line array.
11. After a file set has been created, it is moved into the output data group and, optionally, made available for retrieval.
12. Repeats steps 1 through 11 for any remaining blocks of data.

13. After a file has been successfully processed, it writes created files sets and their temporary cache files to the Report Management path specified in system settings. (See "To configure local settings" on page 60 to set this path.)
14. After the file set is completed, it is copied into a data group and removed from this location. Processed files are copied to either the **Successfully Processed** or **Failed to Process** directories under this path. The contents of the source files are not modified in any manner. Any errors that occur during processing are logged to the Report Management Error Log. (See "Report Management Errors" below for more information.)

Report Management Errors

Administrators can view Report Management Errors for all Report Management Jobs for their entity. When the job is processed, any errors that occur are written to the Report Management Error Log.



NOTE

You can perform tasks for Report Management Errors at the global level and the entity level. Performing tasks at the global level lets you work with Report Management errors for all entities.

To view Report Management Errors

1. After you have logged in to the Administration Console, do one of the following:
 - To work at the global level, on the left pane expand **Global Administration**.
 - To work at the entity level, on the left pane, expand **Entities**, and then expand the appropriate entity.
2. Click **Report Management Errors**.

The right pane shows for each Report Management Error the:

- Date and time the error occurred
- Entity ID (Only if accessed under Global Administration.)
- Name of the job
- Workstation on which the error occurred
- Name and location of the source file

To delete Report Management Errors for a date range

1. After you have logged in to the Administration Console, do one of the following:
 - To work at the global level, on the left pane expand **Global Administration**.
 - To work at the entity level, on the left pane, expand **Entities**, and then expand the appropriate entity.
2. Click **Report Management Errors**.
3. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Delete Range**.
 - On the toolbar, click **Delete Range**.
 - Right-click the selected item, and then click **Delete Range**.

4. In the **Delete Error Log Range** dialog box, type the date range, and then click **OK**.
5. Click **Yes** to confirm the deletion.

To export Report Management Errors for a date range to an XML file

1. After you have logged in to the Administration Console, do one of the following:
 - To work at the global level, on the left pane expand **Global Administration**.
 - To work at the entity level, on the left pane, expand **Entities**, and then expand the appropriate entity.
2. Click **Report Management Errors**.
3. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Export Range**.
 - On the toolbar, click **Export Range**.
 - Right-click the selected item, and then click **Export Range**.
4. In the **Export Error Log Entry Range** dialog box, type the date range, and then click **OK**.
5. In the **Export Error Log Entries** dialog box, confirm that the date range is correct, and then click **Yes**.
6. In the **Export Log** dialog box, select the location where the export file will go.
7. In the **File Name** box, type a name for the export file, and then click **Save**.

To refresh the list of Report Management Errors

1. After you have logged in to the Administration Console, do one of the following:
 - To work at the global level, on the left pane expand **Global Administration**.
 - To work at the entity level, on the left pane, expand **Entities**, and then expand the appropriate entity.
2. Click **Report Management Errors**.
3. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Refresh**.
 - On the toolbar, click **Refresh**.
 - Right-click the selected item, and then click **Refresh**.

To delete Report Management Errors

1. After you have logged in to the Administration Console, do one of the following:
 - To work at the global level, on the left pane expand **Global Administration**.
 - To work at the entity level, on the left pane, expand **Entities**, and then expand the appropriate entity.
2. Click **Report Management Errors**.
3. On the right pane, click the item(s) to delete (hold down the Ctrl key to select multiple items), and then do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Delete Selected Item(s)**.
 - On the toolbar, click **Delete Selected Item(s)**.
 - Right-click the selected item(s), and then click **Delete Selected Item(s)**.

4. Click **Yes** to confirm the deletion.

To export Report Management Errors to an XML file

1. After you have logged in to the Administration Console, do one of the following:
 - To work at the global level, on the left pane expand **Global Administration**.
 - To work at the entity level, on the left pane, expand **Entities**, and then expand the appropriate entity.
2. Click **Report Management Errors**.
3. On the right pane, click the item(s) to delete (hold down the Ctrl key to select multiple items), and then do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Export Selected Item(s)**.
 - On the toolbar, click **Export Selected Item(s)**.
 - Right-click the selected item(s), and then click **Export Selected Item(s)**.
4. Click **Yes** to confirm the export.
5. In the **Export Log** dialog box, select the location where you the export file will go.
6. In the **File Name** box, type a name for the export file, and then click **Save**.

To view the properties of a Report Management Errors

1. After you have logged in to the Administration Console, do one of the following:
 - To work at the global level, on the left pane expand **Global Administration**.
 - To work at the entity level, on the left pane, expand **Entities**, and then expand the appropriate entity.
2. Click **Report Management Errors**.
3. On the right pane, select the item to view, and then do one of the following:
 - Double-click the selected item.
 - On the **Action** menu, point to **All Tasks**, and then click **Properties**.
 - On the toolbar, click **Properties**.
 - Right-click the selected item(s), and then click **Properties**.

CHAPTER 9

WorkFlow

WorkFlow Overview	258
Terms You Should Know	258
Plan Your Workflow	260
Worksteps Overview	261
WorkFlow Definitions	266
Configure Workflow Definitions	268



Workflow Overview

Workflow is an optional, separately licensed component of the PaperVision Enterprise product suite that adheres to the standards prescribed by the Workflow Management Coalition (WFMC). Workflow administrators can use Workflow to define a set of procedural steps that automate business processes. Workflow administrators define, manage, and monitor all workflow designs and instances through the PaperVision Enterprise Administration Console. (Workflow administrators do not have access to documents or functions in any projects unless a global administrator has granted access to those items.)

See the following related sections for more information:

- See "Terms You Should Know" below for a list of terms and definitions that are used throughout the Workflow documentation.
- See "Plan Your Workflow" on page 260 for information that is useful in planning your workflow.
- See "Workflow Definitions" on page 266 for information about using the Workflow Designer.
- See "Configure Workflow Definitions" on page 268 for information about building a workflow definition.

Terms You Should Know

This content contains definitions for terms that are used throughout the Workflow documentation and online help. Knowing this terminology will help you use Workflow and its documentation more effectively. These are standard terms, or approved synonyms prescribed by the Workflow Management Coalition (WFMC).

- See "Workflow" below for a definition of this term.
- See "Workflow Definition" on the facing page for a definition of this term.
- See "Workflow Instance" on the facing page for a definition of this term.
- See "Pre-Conditions" on the facing page for a definition of this term.
- See "Workstep Definition" on the facing page for a definition of this term.
- See "Workstep Instance" on the facing page for a definition of this term.
- See "Workstep Owner" on the facing page for a definition of this term.
- See "Workstep Participant" on page 260 for a definition of this term.
- See "Task" on page 260 for a definition of this term.
- See "Workstep Transition" on page 260 for a definition of this term.
- See "Post-Condition" on page 260 for a definition of this term.

Workflow

A workflow is the automation of a business process in which documents, information, or tasks are passed from one participant to another, according to a set of rules.

Workflow Definition

A workflow definition describes a series of activities (workstep definitions), and the order and conditions under which they execute, that are controlled by the automation service to automate a business process.

Workflow Instance

A workflow instance is a single enactment of a workflow definition. When a document is imported into PaperVision Enterprise, the automation service will evaluate the document against all workflow pre-conditions. Every document that meets a pre-condition will spawn a workflow instance of a workflow definition. For example, if you create a workflow definition for a loan processing application that is based on the initial loan document, a workflow instance is created every time a loan document is imported that meets the pre-conditions you defined. A single document can be active in multiple workflow instances at the same time. If the document is deleted, the workflow instance is transitioned to the end automatically, and the workflow history entry states that the document was deleted.

Pre-Conditions

Pre-Conditions define a set of rules based on document index criteria that are used to determine if a document will spawn a new workflow instance when it is imported, or manually added to a project. You can also evaluate existing documents in a project against pre-conditions. A workflow definition can contain multiple pre-conditions. When a document is added, a workflow instance is created once a pre-condition is met, and none of the remaining pre-conditions are evaluated. If no pre-conditions are defined for a workflow definition, administrators, and users with appropriate permissions can manually create workflow instances.

Workstep Definition

A workstep definition describes an activity that forms one logical step within a workflow definition. These activities can consist of a series of tasks that a user must perform, or can be automated and completed by the automation service. Worksteps must be completed in the order defined in the workflow definition. Worksteps can be manual, where a workstep participant takes ownership of the workstep; automated, where the automation service takes ownership of the workstep; or custom code, where the PaperVision Custom Code Server takes ownership of the workstep.

Workstep Instance

A workstep instance is the enactment of the current workstep definition within a workflow instance. There is only one workstep instance of a workstep definition at a time. A workstep instance can be owned by a single user, or unowned. A workstep instance does not need to be completed all at once. If a workstep instance contains multiple tasks, a user can complete a task, leave the workstep instance, and return later to complete the remaining tasks.

Workstep Owner

As workstep instances are created, they are made available for any of the defined workstep participants to take ownership. At this point, the specific user (or automation service) that maintains ownership of the workstep instance is known as the workstep owner. Once a user takes ownership of a workstep

instance, no other participant can perform any of the tasks for that workstep instance. Ownership of a workstep instance can only be revoked by an administrator.

Workstep Participant

A workstep participant is a resource such as a user, or group of users, that performs tasks within a workstep instance.

Task

A task is an item of work that must be performed in a workstep instance. Since a workstep can only be owned by a single user, all of the tasks within that workstep must be performed by that workstep owner. Tasks within a workstep do not have to be performed in any specific order. However, you can specify the order that the tasks are presented to the user.

Manual tasks are completed by the workstep owner. Automated tasks are performed by the automation service, and can include sending email messages, launching separate applications, changing an index value, and executing command line instructions.

Workstep Transition

A workstep transition takes place when the post-conditions in a workstep are met, and the workflow instance transitions to the next workstep.

Post-Condition

A post-condition is a rule that defines when a workstep instance is complete. A workstep definition can have multiple post-conditions, but the workstep will transition as soon as a single post-condition is met.

Plan Your Workflow

WorkFlow can support large, complex workflows. For best results, fully plan and define the business process that you want to automate before you begin building the workflow. Answering the following questions before you begin may help you with your workflow design.

- What is the scope of the business process you want to automate?
- What do you want to accomplish with the workflow?
- What steps must be performed to complete the entire business process?
- Who performs those steps?
- What tasks must be completed in those steps?
- What must happen before each step is completed and ready for the next step to begin?
 - Is there a decision to be made to determine which step is next (decision routing)?
 - Are there tasks that must be finished (completion routing)?
 - Are there document index criteria that must be met (calculated value routing)?
- What will initiate a new workflow?
- Do all documents being added to a project need to be processed, or only specific documents?

Worksteps vs Tasks

When building workflows, administrators sometimes have difficulty determining whether an operation should be a workstep, or simply a task. The following guidelines may help you make that decision.

- If operations must be completed in a specific order, then they must be separated into worksteps. This is necessary because tasks can be completed in any order.
- If the operations must be completed by separate groups of users, those operations should be separate worksteps.
- If there is a benefit (processing time, cost, etc.) in splitting multiple operations across multiple users, you should separate the operations into individual worksteps. This is necessary because only a single user can perform all the tasks in a specific workstep instance.

Worksteps Overview

Understanding how and when worksteps are processed and transitioned will help you better design your workflow definition. Automated, manual, and custom code worksteps are processed differently.

- See "Automated Worksteps" below for more information.
- See "Manual Worksteps" on the next page for more information.
- See "Custom Code Worksteps" on the next page for more information.

Automated Worksteps

Automated worksteps use the automation service as a workstep participant. The **Workflow (Automated)** setting must be enabled for the automation service. See "Configure Automation Service Scheduling" on page 61 for information on setting this option. When the service runs, the following events occur.

1. The automation service retrieves a list of all unowned automated workstep instances.
2. The service loads the workflow definition of the first workstep instance.
3. The service then takes ownership of the workstep so that other automation services processing workflow instances do not try to run the same workstep instance.
4. The post-conditions of the workstep are evaluated to determine if the workstep should be transitioned. If a post-condition is met, the workstep is transitioned to the next appropriate workstep.
5. If no post-conditions are met, the service then processes the first task in the workstep.
6. Steps 4 and 5 are repeated until there are either no more tasks to process or a post-condition is met. If there are no remaining tasks to process, and no post-conditions have been met, the service will transition the workstep to a Stop/End state, finalizing the workflow.
7. Steps 2 through 6 are repeated until all of the worksteps have been processed.
8. The service then repeats steps 1 through 7 for any remaining entities.

Manual Worksteps

When a workstep owner accesses an owned workstep instance, the following events occur.

1. The automation service processes the workstep to determine if any post-conditions are already met. If so, the workstep is completed and the service transitions the workflow to the next workstep.
2. If no post-conditions have been met, the service determines if the next listed task is an automated task (such as executing a command-line operation). If it is an automated task, the service executes the task, and then repeats steps 1 and 2 until there are no automated tasks next in line.
3. The workstep owner then marks a manual task as complete.
4. The automation service then processes the workstep to determine if any post-conditions have been met. If so, the workstep is completed and the service transitions the workflow to the next workstep.
5. If no post-conditions have been met, the service determines if the next listed task is an automated task (such as executing a command-line operation). If it is an automated task, the service executes the task, and then repeats steps 4 and 5 until there are no automated tasks next in line.
6. Steps 3 through 5 are repeated until a post-condition is met, and the workflow transitions to the next workstep.

Custom Code Worksteps

Custom code worksteps are treated as manual worksteps by the automation service because the service does not execute the custom code.

1. The PaperVision custom code server accesses PaperVision Enterprise as a workstep participant, and retrieves any workstep instances that are waiting to be processed by that participant's group.
2. Custom code worksteps have a single task: execute the custom code.
3. The custom code server executes the custom code. The workstep transition is specified in the custom code.
4. The automation service marks the workstep as complete and transitions the workstep.

WorkFlow Custom Code Server

You must download and configure the PaperVision Enterprise WorkFlow Custom Code Server for automated custom code worksteps to process. The PaperVision Enterprise WorkFlow Custom Code Server acts as the workstep participant for custom code steps. You can install this server on the PaperVision Enterprise Server, or any computer on your network (or the internet) that can communicate with the PaperVision Enterprise Server. You can install multiple WorkFlow Custom Code Servers. Each WorkFlow Custom Code Server installation can run multiple workstep instances simultaneously. You can also install multiple WorkFlow Custom Code Servers to further increase the number of custom code worksteps that can be run simultaneously.

The PaperVision Enterprise WorkFlow Custom Code Server is comprised of the following components.

- **PaperVision Enterprise WorkFlow Custom Code Server Configuration tool** - Administrators can manage the PaperVision Enterprise WorkFlow Custom Code Server through the configuration tool. You can configure the number of worker instances that are spawned at once, and specify which worksteps each worker will process. The configuration tool also displays what each worker is currently processing (see " WorkFlow Custom Code Server Configuration Tool" on the next page for information about configuring workers).
- **PaperVision WorkFlow Initiator Service** - This Windows service spawns workflow workers that communicate with the PaperVision Enterprise Server, take ownership of each workstep instance waiting to be processed, and then execute the custom code for that workstep. To keep from downloading the custom code repeatedly, the worker maintains a local encrypted cache of the defined custom code. If no custom code is currently cached, the worker will download the custom code. If an administrator changes the custom code, the worker automatically detects the change and retrieves the updated custom code. This service checks for instances to process every 5 minutes.

To download the PaperVision Custom Code Server

1. In the PaperVision Enterprise User Console, on the title bar, click the down arrow next to your user name, and then click **Downloads**.
2. In the **PaperVision Enterprise WorkFlow Custom Code Server** area, click **Download**.
3. Click **Run** to open the **PaperVision WorkFlow Custom Code Server - InstallShield Wizard**, and then click **Next**.
4. Click **Yes** to accept the end user license agreement, and then click **Install**.
5. Click **Finish** to complete the installation.

To change the WorkFlow Initiator Service interval

1. On the server where the service is installed, open the folder located at: **C:\Program Files (x86)\Digitech Systems\PaperVision\WorkFlow Custom Code Server**.
2. Double-click the **DSI.PVECommon.WorkFlowServer.PVWorkFlowInit.exe.config** file. If you are prompted to do so, open the file in Microsoft Notepad.
3. Under the **SERVER SETTINGS** heading, find the following code:


```
processStartIntervalMilliseconds="60000"
```

This code specifies a default process interval value of 60,000 milliseconds, or 5 minutes.
4. Change the interval value, in milliseconds, to the time you specify.
5. On the toolbar, click **File**, and then select **Save**.
6. Close Microsoft Notepad.
7. Restart the **PaperVision WorkFlowInitiator1** service.

Workflow Custom Code Server Configuration Tool

Once you have downloaded the Workflow Custom Code Server, you can access the configuration tool from the programs directory. The configuration tool displays which custom code workstep each server process instance is configured to execute. The Custom Code Server can spawn one or more worker processes to process worksteps. Each of the worker processes is a new instance of the worker, and operates independently of the others. The more worker processes configured to run, the more system resources (memory and processor) are used. Therefore, you may want to limit the number of processes that the server uses if the computer is used for purposes other than running the Custom Code Server. The optimal number of processes is determined by the custom code you select to run in each configured workstep. On a multi-use system (being used for other purposes) it is recommended to start with one or two processes, and then increase the count as you monitor performance. For single-use systems (systems used as only a Custom Code Server), you should start with eight processes, and then increase or decrease the count as desired.

To specify the number of processes running on the Workflow Custom Code Server

1. From the **Programs** directory, open the **PaperVision Workflow Custom Code Configuration** tool.
2. On the toolbar, click **Server Settings** to open the **Server Settings** dialog box.
3. In the **Instance Settings** box, increase or decrease the number of **Simultaneous Processes** to the desired number.
4. Click **OK**, and then click **Yes** to restart the service.

To specify the worksteps processed by a worker instance



TIP

You can configure each instance of a worker to process one or more worksteps. You can also configure multiple instances to process the same workstep to complete it faster. When a worker instance starts, it iterates through its list of defined worksteps. For each workstep, it processes every workstep instance in the queue before it moves on to the next workstep. After all the worksteps are completed, the worker waits for the specified interval before it starts the process over.

1. From the **Programs** directory, open the **PaperVision Workflow Custom Code Configuration** tool.
2. On the toolbar, in the **Instance** box, click the down arrow to open the **Instance** list, and select the worker instance that you want to configure. A list of worksteps defined for that worker instance appears.
3. On the toolbar, click **Add Workstep** to open the **Custom Code Server Configuration Login** dialog box. Specify the following:
 - In the **Server URL** box, type the URL of the PaperVision Enterprise Server.
 - In the **Entity ID** box, type the entity ID for your user account.
 - Type the user name and password for a user that is a member of the group that is defined as the workstep participant (Custom Code Server group) in the workstep definition.

4. Click **OK** to open a list of the specified user's workflows and custom code worksteps.
5. Select the worksteps you want to assign to the worker instance, and then click **OK**.
6. (Optional) You can change the order in which worksteps are processed. From the list, select the workstep for which you want to change the priority. On the toolbar, use the **Move Up** and **Move Down** arrows to change the order in which the worksteps are processed.
7. (Optional) To remove a workstep, select the workstep from the list, and then click **Delete**.
8. (Optional) To change the user settings for a workstep, select the workstep from the list, and then, on the toolbar, click **Change User Settings**. Type the new user name and password.
9. (Optional) To view all of the worksteps for all of the server instances, on the toolbar, select **Show All**.
10. Click **Save** to save your settings.

To copy a worker instance



T I P

You can copy a worker instance to another instance to double the throughput. Any configuration settings in the destination instance are overwritten with the new settings.

1. From the **Programs** directory, open the **PaperVision WorkFlow Custom Code Configuration** tool.
2. On the toolbar, in the **Instance** box, click the down arrow to open the **Instance** list, and select the worker instance that you want to copy.
3. On the toolbar, click **Copy Instance Settings**.
4. In the **Copy Instance Settings** dialog box, select the destination instance from the list.
5. Click **OK**, and then click **Yes**.

To view the WorkFlow Custom Code Server status

1. From the **Programs** directory, open the **PaperVision WorkFlow Custom Code Configuration** tool.
2. On the toolbar, click **Server Status** to open the **Custom Code Server Status** window. The window lists each server instance, its current state, and current operation.
3. (Optional) To stop a server instance, select the instance from the list, and then do one of the following:
 - On the toolbar, click **Stop**.
 - Right-click the server instance, and then select **Stop**.
4. (Optional) To start a server instance, select the instance from the list, and then do one of the following:
 - On the toolbar, click **Start**.
 - Right-click the server instance, and then select **Start**.
5. (Optional) To refresh the list, on the toolbar, click **Refresh**.

Workflow Definitions

Workflow administrators can define workflows graphically, without any programming or scripting, in the **Workflow Designer**. (See "Configure Workflow Definitions" on page 268 for instructions.) Under **Workflow Definitions**, you can access functions to manage existing workflow definitions and create new ones.

To view workflow definitions

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Projects**.
3. Expand the appropriate project, and then click **Workflow Definitions**.

The right pane shows for each workflow definition the:

- Name of the workflow definition
- Whether the workflow definition is active

To add a new workflow definition

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Projects**.
3. Expand the appropriate project, and then click **Workflow Definitions**.
4. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **New Workflow**.
 - On the toolbar, click **New**.
 - Right-click the selected item, and then click **New Workflow**.
5. In the **New Workflow** dialog box, specify the following items:
 - In the **Workflow Name** box, type the name of the new workflow definition.
 - Click the down arrow in the **Project Name** box, and then select the project to assign to the new workflow definition.
6. Click **OK** to open the **Workflow Designer**.
7. See "Configure Workflow Definitions" on page 268 for instructions to configure the workflow definition.

To refresh the list of workflow definitions

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Projects**.
3. Expand the appropriate project, and then click **Workflow Definitions**.
4. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Refresh**.
 - On the toolbar, click **Refresh**.
 - Right-click the selected item, and then click **Refresh**.

To delete workflow definitions



NOTE

When you delete a workflow definition, and click **Save All Workflows**, the workflow definition and all workflow instances of that definition (both completed and in progress) are removed. The workflow history and status for the deleted workflow are removed (any archived workflow history reports that you created are still available).

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Projects**.
3. Expand the appropriate project, and then click **WorkFlow Definitions**.
4. On the right pane, select the workflow definition(s) to delete (hold down the Ctrl key to select multiple items), and then do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Delete**.
 - On the toolbar, click **Delete**.
 - Right-click the selected item, and then click **Delete**.
5. To confirm the deletion, click **Yes**.

To edit the properties of a workflow definition



NOTE

Any modifications you make to workflow definitions, workstep tasks, and post-conditions take place when you save the workflow definition. When you delete a workstep definition and save your changes, it is immediately removed. Existing workstep instances are processed, but no new workstep instances for the deleted workstep definition will be created.

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **Projects**.
3. Expand the appropriate project, and then click **WorkFlow Definitions**.
4. On the right pane, select the workflow definition, and then do one of the following:
 - Double-click the selected item.
 - On the **Action** menu, point to **All Tasks**, and then click **Properties**.
 - On the toolbar, click **Properties**.
 - Right-click the selected item, and then click **Properties**.
5. In the **WorkFlow Definition Properties** window, you can make changes to the workflow definition. (See "Configure Workflow Definitions" on the next page for information about the settings.)

Configure Workflow Definitions

We recommend the following sequence when building your workflow definition.

1. Create the necessary user groups. (See "System Groups" on page 142 for instructions.)
2. Define the criteria that will initiate a workflow instance by adding a pre-condition. (See "To add a pre-condition to a workflow definition" on the facing page for instructions.)
3. Create all the worksteps needed in the workflow. (See "Add Worksteps " on page 272 for instructions.)
4. Link all of the worksteps in the order needed to define the business process. (See "Link Worksteps" on page 275 instructions.)
5. Define all the tasks and post conditions for each workstep. (See "Add Tasks" on page 277, and "Add Post-Conditions" on page 279 for instructions.)



NOTE

Any modifications you make to existing workflow definitions, workstep tasks, and post-conditions take place when you save the workflow definition. When you delete a workstep definition and save your changes, it is immediately removed. Existing workstep instances are processed, but no new workstep instances for the deleted workstep definition will be created.

To open the WorkFlow Designer



NOTE

You can open the **WorkFlow Designer** by performing the steps to either edit an existing workflow or add a new one.

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
 2. Expand the appropriate entity, and then expand **Projects**.
 3. Expand the appropriate project, and then click **WorkFlow Definitions**.
 4. Do one of the following:
 - To open the **WorkFlow Designer** by editing an existing workflow, on the right pane, double-click a workflow definition.
 - To open the **WorkFlow Designer** by adding a workflow, do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **New WorkFlow**.
 - On the toolbar, click **New**.
 - Right-click the selected item, and then click **New WorkFlow**.
1. In the **WorkFlow Name** box, type the name of the new workflow definition.
 2. Click the down arrow in the **Project Name** box, and then select the project to assign to the new workflow definition.
 3. Click **OK** to open the **WorkFlow Designer**.

To configure a workflow definition

1. If you have not already done so, open the **WorkFlow Designer**. (See "To open the WorkFlow Designer" on the previous page if you need instructions.)
2. (Optional) To create a new workflow definition from the **WorkFlow Designer**, on the **Home** ribbon, click **Add Item**, and then select **Add WorkFlow**. In the **New WorkFlow** dialog box, specify the following:
 - In the **WorkFlow Name** box, type the name of the new workflow definition.
 - Click the down arrow in the **Project Name** box, and then select the project to assign to the new workflow definition.
3. On the left pane, select the workflow to configure.
4. (Optional) On the right pane, in the **Description** box, type a description of the workflow.
5. You must define at least one pre-condition to determine what documents in a project will initiate a workflow instance. See "To add a pre-condition to a workflow definition" below for instructions.
6. Add the necessary worksteps to your workflow definition. Worksteps can be manual, automated, or custom code.
 - See "To add a manual workstep" on page 274 for instructions.
 - See "To add an automated workstep" on page 272 for instructions.
 - See "To add a custom code workstep " on page 273 for instructions.
7. After you have added all the worksteps you need, you must link the worksteps in the order that you want defined in your workflow definition. See "Link Worksteps" on page 275 for instructions.
8. Add the tasks to be completed for each workstep. (Tasks are not needed for custom code worksteps.) See "Add Tasks" on page 277 for instructions.
9. Add the post-conditions for each workstep. (Post-conditions define when a workstep is completed and can transition to the next workstep.) See "Add Post-Conditions" on page 279 for instructions.
10. Verify the workflow. See "Verify Workflows" on page 283 for instructions.
11. On the **Home** ribbon, click **Save All Workflows** to open the **Save Workflow(s)** dialog box.
12. In the **Select** column, select the workflow definitions to save, and then click **Save**.

To add a pre-condition to a workflow definition



NOTE

A pre-condition is a set of rules that you define to determine which documents will initiate a workflow instance. You can specify whether you want all existing documents in a project evaluated against your pre-condition, or only new documents (or new versions of documents) that are added to the project.

1. If you have not already done so, open the **WorkFlow Designer**. (See "To open the WorkFlow Designer" on the previous page if you need instructions.)
2. On the left pane, select the workflow to configure.

3. Do one of the following:
 - On the **Home** ribbon, click **Add Item**, and then select **Add Pre-Condition**.
 - Right-click the workflow, and then select **Add Pre-Condition**.
4. On the right pane, under **General**, specify the following properties.
 - **Description** - (Optional) Type any information to include that describes the pre-condition.
 - **Name** - Type the name of the pre-condition.
5. Under **Search**, and then **Document Selection Method**, specify the following properties.
 - **Criteria for Automated WorkFlow (Pre-Condition)** - To select this option, click the down arrow, and then select **True**. When the WorkFlow (Pre-Condition) automation service runs, it looks for all workflow definitions that have this option set to **True**. Any document in the project that meets the specified search criteria for those workflow definitions will initiate a workflow instance. Those documents are then tagged so that they do not initiate duplicate workflow instances the next time the automation service runs. Additionally, the automation service will look for any index field in the project that has the **WorkFlow Trigger** option selected (see "To add document index fields" on page 163 for more information). If this index has been modified since the last time the automation service ran, the document will initiate a workflow instance for each workflow definition in the project that has **Criteria for Automated WorkFlow (Pre-Conditions)** set to **True**.

**NOTE**

Selecting **Criteria for Automated WorkFlow (Pre-Condition)**, and **New Documents** in the same pre-condition may produce duplicate workflows. When a document that meets the search criteria is added to a project and the **New Documents** option is selected, it will initiate a workflow instance, but is not tagged for the automation service. If the **Criteria for Automated WorkFlow (Pre-Condition)** option is also selected, when the automation service runs, that document will initiate a duplicate workflow instance.

- **New Documents** - To select this option, click the down arrow, and then select **True**. When this option is set to **True**, documents that meet the specified search criteria will initiate a workflow instance when they are added to the project.
-

**NOTE**

You may create duplicate workflow instances if you import a data group and select the **Full/Reload** import type instead of **Append** (see "To set the default import type" on page 80 for more information), and the project already has documents in an existing workflow instance.

- **New Versions** - To select this option, click the down arrow, and then select **True**. When this option is set to **True**, new versions of a document that meet the search criteria will initiate a workflow instance when a user checks in the new version.
6. In the **Search Criteria** box, click the ellipses button to display each index field defined in the project.

7. In the index field boxes, type the criteria that must be met by a document to initiate a workflow instance.

**T I P**

You can type an asterisk (*) in a single index field to specify that all documents in the project meet your search criteria and will initiate a workflow instance.

8. (Optional) In the **Search Type** box, click the down arrow, and then select the operator to apply to the search criteria.
9. (Optional) Click **Test Criteria** to test the search criteria.
10. (Optional) Click **Clear Criteria** to remove the search criteria.
11. Click **OK** to save the pre-condition.

To import a workflow definition

1. If you have not already done so, open the **WorkFlow Designer**. (See "To open the WorkFlow Designer" on page 268 if you need instructions.)
2. On the **Home** ribbon, in the **Input/Output** group, click **Import**.
3. Select the XML file to import, and then click **Open**.
4. In the **Select Project** dialog box, click the down arrow and then select the project to which you want add the workflow definition.
5. Click **OK**.

**N O T E**

The workflow definition is added to the project you selected. However, you must then configure any document packages, pre-conditions, notification groups, and workstep participants.

To export a workflow definition

1. If you have not already done so, open the **WorkFlow Designer**. (See "To open the WorkFlow Designer" on page 268 if you need instructions.)
2. On the **Home** ribbon, in the **Input/Output** group, click **Export**.
3. Click the file format for the export; you can choose one of the following:
 - XML - This option exports the workflow definition as an XML file that can be imported into PaperVision Enterprise.
 - PDF - This option exports a PDF file of the workflow diagram.
 - PNG - This option exports a PNG file of the workflow diagram.
 - Visio - This options exports a Visio file of the workflow diagram.
4. In the **Save As** dialog box, select the location to where you want the file exported.
5. In the **Name** box, type the name of the file.
6. Click **Save**.

Add Worksteps

Worksteps define the order in which operations in your workflow definition must take place. Worksteps can be manual, where a workstep participant takes ownership of the workstep; automated, where the automation service takes ownership of the workstep; or custom code, where the PaperVision Enterprise Custom Code Server takes ownership of the workstep.

To add an automated workstep

1. If you have not already done so, open the **WorkFlow Designer**. (See "To open the WorkFlow Designer" on page 268 if you need instructions.)
2. On the left pane, select the workflow.
3. Do one of the following:
 - Right-click the workflow, point to **Add**, and then **Add Workstep**, and then click **Automated**.
 - On the **Home** ribbon, click **Add Item**, point to **Add Workstep**, and then click **Automated**.
 - On the **Home** ribbon, click **Designer**. Right-click the right pane, point to **Add Workstep**, and then click **Automated**.

An automated workstep is added to the workflow you selected.

4. On the right pane, specify the following workstep properties.
 - **Description** - (Optional) Type any information you want to include in a description of the automated workstep.
 - **Graphic** -(Optional) You can specify the graphic used for the workstep in the designer. In the **Graphic** box, click the ellipses button to open the **WorkStep Graphic** dialog box. Select the graphic to use, and then click **OK**.
 - **Initial workstep** - If this is the first workstep in the workflow, click the down arrow, and then select **True**. If this is not the first workstep in the workflow, select **False**.
 - **Name** - Type the name of the automated workstep.
5. (Optional) On the left pane, you can right-click the automated workstep to access the following editing options:
 - **Cut** - Removes the workstep from the workflow and places it on the clipboard.
 - **Copy** - When you click **Copy**, you can select **Copy Workstep** to copy only the workstep to the clipboard or select **Copy Workstep and its children** to copy the workstep, its tasks, and post-conditions to the clipboard.
 - **Paste** - Adds the contents of the clipboard to the workflow.
 - **Delete** - Removes the workstep.
 - **Convert to Manual** - Converts the automated workstep to a manual workstep. This removes any automated-specific post-conditions. You can then assign the proper tasks, post-conditions, and participants.

6. Repeat this procedure for all the automated worksteps you need in the workflow.

**T I P**

You can create an automated workstep with no tasks that will act as a holding step. Create a post-condition and configure the **Workstep Completion** property to specify the worksteps to be completed before transitioning to the next workstep. To prevent over filling the history logs, no logs are generated while an item is in the holding step.

To add a custom code workstep

**N O T E**

For custom code worksteps to process, you must configure the WorkFlow Custom Code Server and turn on the automation service. See "WorkFlow Custom Code Server" on page 262 for more information.

1. If you have not already done so, open the **WorkFlow Designer**. (See "To open the WorkFlow Designer" on page 268 if you need instructions.)
2. On the left pane, select the workflow.
3. Do one of the following:
 - Right-click the workflow, point to **Add**, and then **Add Workstep**, and then click **Custom Code**.
 - On the **Home** ribbon, click **Add Item**, point to **Add Workstep**, and then click **Custom Code**.
 - On the **Home** ribbon, click **Designer**. Right-click the right pane, point to **Add Workstep**, and then click **Custom Code**.

A custom code workstep is added to the workflow you selected.

4. On the right pane, specify the following **General** properties.
 - **Description** - (Optional) Type any information you want to include in a description of the custom code workstep.
 - **Initial workstep** - If this is the first workstep in the workflow, click the down arrow, and then select **True**. If this is not the first workstep in the workflow, select **False**.
 - **Name** - Type the name of the custom code workstep.
5. In the **Custom Code Script** box, click the ellipses button to open the **Select Custom Code Generator** dialog box, and then do the following:
 1. In the **Language** box, click the down arrow, and then select the programming language to use.
 2. Select the **Basic** script, and then click **OK** to open the **Script Editor**.
 3. Edit the available script, or insert your own code, and then click **OK**.
6. In the **Custom Code Server User** box, click the ellipses button, and then select the group for the custom code server to use as a workstep participant. (See "WorkFlow Custom Code Server" on page 262 for more information about the workflow custom code server.)

7. (Optional) On the left pane, you can right-click the custom code workstep to access the following editing options:
 - **Cut** - Removes the workstep from the workflow and places it on the clipboard.
 - **Copy** - Copies the workstep to the clipboard.
 - **Paste** - Adds the contents of the clipboard to the workflow.
 - **Delete** - Removes the workstep.
8. Repeat this procedure for all of the custom code worksteps that you need.

To add a manual workstep

1. If you have not already done so, open the **WorkFlow Designer**. (See "To open the WorkFlow Designer" on page 268 if you need instructions.)
2. On the left pane, select the workflow.
3. Do one of the following:
 - Right-click the workflow, point to **Add**, and then **Add Workstep**, and then click **Manual**.
 - On the **Home** ribbon, click **Add Item**, point to **Add Workstep**, and then click **Manual**.
 - On the **Home** ribbon, click **Designer**. Right-click the right pane, point to **Add Workstep**, and then click **Manual**.

A custom code workstep is added to the workflow you selected.

4. On the right pane, specify the following **General** properties.
 - **Description** - (Optional) Type any information you want to include in a description of the manual workstep.
 - **Graphic** - (Optional) You can specify the graphic used for the workstep in the designer. In the **Graphic** box, click the ellipses button to open the **WorkStep Graphic** dialog box. Select the graphic to use, and then click **OK**.
 - **Initial workstep** - If this is the first workstep in the workflow, click the down arrow, and then select **True**. If this is not the first workstep in the workflow, select **False**.
 - **Name** - Type the name of the manual workstep.
 - **Workstep Participant** - Click the ellipses button, and then select the user group to assign as a workstep participant to the workstep.
5. Under **Time Limit for Uncompleted Worksteps (Owned)**, specify the following properties.
 - **Notification Group** - Click the ellipses button in the **Notification Group** box, and then select the group to be notified when the workstep exceeds the maximum time you specify below.
 - **The maximum time (minutes) before notification** - Type the number of minutes (or use the arrows) to specify how long the workstep can remain owned and not completed before the group you specified is notified.
 - **The maximum time (minutes) before transition** - Type the number of minutes (or use the arrows) to specify how long the workstep can remain owned and not completed before it is transitioned to another workstep.
 - **Transition Workstep** - Click the ellipses button, and then select the workstep to which the workflow will transition after the maximum time you specified elapses.

6. Under **Time Limit for Worksteps Waiting in Queue**, specify the following properties.
 - **Notification Group** - Click the ellipses button, and then select the group to be notified when the workstep exceeds the maximum time you specify below.
 - **The maximum time (minutes) before notification** - Type the number of minutes (or use the arrows) to specify how long the workstep can remain in queue before the group you specified is notified.
 - **The maximum time (minutes) before transition** - Type the number of minutes (or use the arrows) to specify how long the workstep can remain in queue before it is transitioned to another workstep.
 - **Transition Workstep** - Click the ellipses button, and then select the workstep to which the workflow will transition after the maximum time you specified elapses.
7. (Optional) On the left pane, you can right-click the manual workstep to access the following editing options:
 - **Cut** - Removes the workstep from the workflow and places it on the clipboard.
 - **Copy** - When you click **Copy**, you can select **Copy Workstep** to copy only the workstep to the clipboard or select **Copy Workstep and its children** to copy the workstep, its tasks, and post-conditions to the clipboard.
 - **Paste** - Adds the contents of the clipboard to the workflow.
 - **Delete** - Removes the workstep.
 - **Convert to Automated** - Converts the manual workstep to an automated workstep. This removes any manual-specific post-conditions and tasks. You can then assign the proper tasks and post-conditions.
8. Repeat this procedure for all of the manual worksteps that you need.

Link Worksteps

Linking worksteps defines how documents move through the workflow definition. You can link worksteps using several different methods. Worksteps are initially linked in the order in which they are added to the workflow definition. For example, if you add three worksteps, the first two worksteps will each have a preliminary post-condition that links them to the next workstep. You can change the workstep to which each one transitions by editing the post-condition (see "Add Post-Conditions" on page 279 for information on post-conditions), or by linking and de-linking the workstep on the **Layout** tab.

To link worksteps on the Layout tab

1. If you have not already done so, open the **WorkFlow Designer**. (See "To open the WorkFlow Designer" on page 268 if you need instructions.)
2. On the left pane, select the workflow for which you want to link worksteps.
3. Click the **Layout** ribbon.
4. On the right pane, select the first workstep to link.

5. Press Ctrl, and then select the destination workstep.
6. On the **Layout** ribbon, in the **Edit** group, click **Link Worksteps**.



NOTE

The worksteps are linked in the order in which you selected them. On the right pane, an arrow from the first workstep you selected, to the destination workstep, shows that the two worksteps are linked. This procedure also updates the post-conditions of the worksteps.

7. (Optional) To remove a link between two worksteps, do the following:
 1. Select the destination workstep.
 2. Press Ctrl, and then click the initial workstep.
 3. On the **Layout** ribbon, in the **Edit** group, click **De-link Worksteps**.
 4. On the right pane, the arrow between the two worksteps is removed, and the post-conditions are updated.
8. Repeat these steps for any links that you want to add or remove.

Custom Code Worksteps

Custom code worksteps are transitioned differently. Because a custom code workstep only executes custom code, there is no post-condition that has to be met to initiate a transition. Instead, transitions are added to custom code worksteps the same way post-conditions are added to other worksteps when you link them. (In some cases, the custom code may define and execute a transition.) The following procedure describes how to add a new transition, or edit an existing one. When working with transitions, keep the following in mind:

- If you have multiple instances of a document in a workflow, and you want to mark this workstep complete without transitioning it, select **No Transition/Only Mark Workstep Complete**, and then click **Add**. This is useful in parallel workflows, where multiple worksteps must be completed before the document is transitioned. For example, if the same document has to be signed by several users before it transitions, this option would keep the worksteps from transitioning until they were all signed.
- Select **Stop/Exit Workflow** to exit the workflow instance. In a parallel workflow, if any one instance of a document hits a **Stop/Exit Workflow** post-condition, all instances of that document will automatically exit the workflow.
- **Transition/Only Mark Workstep Complete**, and **Stop/Exit Workflow** transitions cannot be combined with any other transitions.

To add a Transition to a custom code workstep

1. If you have not already done so, open the **WorkFlow Designer**. (See "To open the WorkFlow Designer" on page 268 if you need instructions.)
2. On the left pane, expand the appropriate workflow, and then select the custom code workstep to which to add a transition.
3. Do one of the following:
 - Right-click the custom code workstep, point to **Add**, and then click **Add Transition**.
 - On the **Home** ribbon, click **Add Item**, and then click **Add Transition**.
4. A transition is added to the custom code workstep you selected.
5. On the right pane, specify the following **General** properties.
 - **Name** - Type the name of transition.
 - **Transitions** - Click the ellipses button to open the **Edit Transitions** dialog box.



NOTE

If the workstep was previously linked, the destination workstep appears in the **Selected Transitions** list on the right.

6. Select the transition from the **Available Transitions** list, and then click **Add**. (Optionally, you can double-click any item in a list to move it to the opposite list.)
7. After you have added or removed the transitions you need, click **OK**.

Add Tasks

A task is an item of work that must be performed in a workstep instance. Manual tasks are completed by the workstep owner. Automated tasks are performed by the automation service, and can include sending email messages, launching separate applications, changing an index value, and executing command line instructions. You can add as many tasks to a workstep as you need.

To add a task

1. If you have not already done so, open the **WorkFlow Designer**. (See "To open the WorkFlow Designer" on page 268 if you need instructions.)
2. On the left pane, select the workflow to which you want to add a task.
3. Do one of the following:
 - Right-click the workflow, point to **Add**, and then click **Add Task**.
 - On the **Home** ribbon, click **Add Item**, and then click **Add Task**.

A task is added to the workstep you selected.

4. On the right pane, specify the following **General** properties.
 - **Description** - (Optional) Type any information you want to include in a description of the task.
 - **Name** - Type the name of the task.
5. Under **Settings**, in the **Task Type** box, click the ellipses button, and then select the task to add.

Use the following table to configure the settings for the task you selected.

Task Type	Task Type Settings
User Operations (Manual Worksteps)	<p>Instructs the user to perform a task. Once the task is completed, the user will click the task, marking it complete.</p> <p>Click the ellipses in the Task Type Settings box to open the User Operations Settings dialog box, and then specify the following:</p> <p>Require Confirmation - Select this option to force the user to click OK in a message box that displays when the task is marked complete.</p> <p>Message - Specify the message or question that appears in the message box.</p>
Launch Application/Shell (Automated and Manual Worksteps)	<p>Causes the server (for automated worksteps), or the user's computer (for manual worksteps) to execute a specified command-line program.</p> <p>Click the ellipses in the Task Type Settings box to open the Launch App Settings dialog box, and then specify the following:</p> <p>Path - Click the ellipses and specify the full path and file name of the command you want to execute, and then click Open.</p> <p>Operation - Click the down arrow, and then select the operation you want to perform from the list.</p> <p>Parameters - Specify the parameter that is passed to the command line when executed.</p>
Raise Event (Automated and Manual Worksteps)	<p>Causes the PaperVision Viewer to raise the WorkstepTaskRequest event. This task is designed for system integrators to integrate task management into third-party applications.</p> <p>Click the ellipses in the Task Type Settings box to open the Raise Event Settings dialog box, and then specify the following:</p> <p>Info Value - Type the information that you want to pass when the event is launched.</p>
Alter Index Values (Manual Worksteps)	<p>Displays the Alter Index Values window in the user console when viewing the document. When the user clicks Save, the task is marked complete.</p>
Send Email (Automated and Manual Worksteps)	<p>Sends an email message to the specified address with the content you configure. See "Email Message Tags" on page 290 for information on configuring email messages.</p>

Task Type	Task Type Settings
Force Index Value (Automated and Manual Worksteps)	<p>Changes an index field to a specified value.</p> <p>Click the ellipses in the Task Type Settings box to open the Force Index Value Settings dialog box, and then specify the following:</p> <p>Field - Click the down arrow, and then select the index field you want to change from the list.</p> <p>Value - Type the value you want to use to populate the specifies index field. See "CURRENTDATETIME Tags" on page 293 for information on using the CURRENTDATETIME tags.</p>
Sign Document (Manual Workstep)	Requires the user to sign the document.
Custom Code (Manual Workstep)	Requires the user to run custom code.
E-Form Validation (Manual Workstep)	Requires the user to save an E-Form. The system performs validation checks when E-Forms are saved.

Add Post-Conditions

Post-conditions define when a workstep is complete. Worksteps can have more than one post-condition. As soon as one post-condition is met, the workflow transitions to the next workstep, and no other post-conditions are evaluated. Default post-conditions are created for any worksteps that you linked together when you built the workflow definition. You can refine or change those post-conditions by using the procedures below.

To add a post-condition to an automated workstep

1. If you have not already done so, open the **WorkFlow Designer**. (See "To open the WorkFlow Designer" on page 268 if you need instructions.)
2. On the left pane, select the workflow to which you want to add a post-condition.
3. Select the automated workstep to which you want to add a post-condition, and then do one of the following:
 - Right-click the workstep, point to **Add**, and then click **Add Post-Condition**.
 - On the **Home** ribbon, click **Add Item**, and then click **Add Post-Condition**.

A post-condition is added to the workstep you selected.

4. On the right pane, specify the following **General** properties.
 - **Name** - Type the name of the post-condition.
 - **Transitions** - Click the ellipses button to open the **Edit Transitions** dialog box.



N O T E

If the workstep was previously linked, the destination workstep appears in the **Selected Transitions** list on the right.

5. Select the transition from the **Available Transitions** list, and then click **Add**. (Optionally, you can double-click any item in a list to move it to the opposite list.)



N O T E

When working with the **Transitions** property, keep the following in mind:

If you have multiple instances of a document in a workflow, and you want to mark this workstep complete without transitioning it, select **No Transition/Only Mark Workstep Complete**, and then click **Add**. This is useful in parallel workflows, where multiple worksteps must be completed before the document is transitioned. For example, if the same document has to be signed by several users before it transitions, this option would keep the worksteps from transitioning until they were all signed.

Select **Stop/Exit Workflow** to exit the workflow instance. In a parallel workflow, if any one instance of a document hits a **Stop/Exit Workflow** post-condition, all instances of that document will automatically exit the workflow.

Transition/Only Mark Workstep Complete, and **Stop/Exit Workflow** transitions cannot be combined with any other transitions.

6. After you have added or removed the needed transitions, click **OK**.
7. Under **Post-Condition Criteria**, specify the following properties.
 - **Document Package** - Configure this option if the workstep requires additional documents before transitioning. This post-condition will search the project for documents that meet the criteria you select before transitioning. For example, if a job application needs additional documents before proceeding, set up the search to look for those items, and once found, the document would move on. To configure this option, click the ellipsis button to open the **Document Package** dialog box, and do the following:
 1. Click **Add Search** to open the **Select Project** dialog box.
 2. In the **Project Name** list, select the project you want to search.
 3. Click **OK** to open the **Search Criteria** dialog box.
 4. Type your search criteria in the index fields.
 5. (Optional) Click the down arrow in the **Search Type** box, and then select the operator to apply to the index fields.
 6. (Optional) If you want to specify the number of documents that must exist in the document package, use the up and down arrows in the **Number of documents that must exist** area, to specify the number you want.

7. (Optional) Click **Test Criteria** to verify your search criteria.
 8. (Optional) Click **Clear Criteria** to remove your entries.
 9. Click **OK** to save your search.
 10. Repeat the procedure for any other document searches you want to add to the document package.
 11. When you are finished, on the **Document Package** dialog box, click **Close**.
- **Document Signed** - To require that a document is signed before the post-condition is met, click the down arrow, and then select **True**.
 - **Tasks** - To require that tasks in the workstep are completed before the post-condition is met, click the ellipses button to open the **Task** dialog box, select the required tasks, and then click **OK**.

**N O T E**

If an automated step has a task selected as a post-condition, and that task has not been completed, the document will exit the workflow immediately. This can produce unexpected behavior.

- **Workflow Instance Document** - To specify that a document exists before the post-condition is met, click the ellipses button to open the **Search Criteria** dialog box.
 1. In the index field boxes, type your search criteria that the document index values must meet.
 2. (Optional) In the **Search Type** box, click the down arrow, and then select the operator to apply to the search criteria.
 3. (Optional) Click **Test Criteria** to test the search criteria.
 4. (Optional) Click **Clear Criteria** to remove the search criteria.
 5. Click **OK** to save the search.
 - **Workstep Completion** - To specify that other worksteps must be completed before the post-condition is met, click the ellipses button to open the **Select Workstep(s)** dialog box. Select the worksteps from the **Available Worksteps** list, and then click **Add**. (Optionally, you can double-click any item in a list to move it to the opposite list.) After you have added or removed the worksteps you need, click **OK**.
8. Under **Post-Condition Order**, set the following property.
 - **Evaluate Remaining Post-Conditions** - For the workstep to transition after all post-conditions are met, select **True**. For the workstep to transition when the first post-condition is met, select **False**.

To add a post-condition to a manual workstep

1. If you have not already done so, open the **WorkFlow Designer**. (See "To open the WorkFlow Designer" on page 268 if you need instructions.)
2. On the left pane, select the workflow to which you want to add a post-condition.
3. Select the manual workstep to which you want to add a post-condition, and then do one of the following:
 - Right-click the workstep, point to **Add**, and then click **Add Post-Condition**.
 - On the **Home** ribbon, click **Add Item**, and then click **Add Post-Condition**.

A post-condition is added to the workstep you selected.

4. On the right pane, specify the following **General** properties.
 - **Name** - Type the name of the post-condition.
 - **Transitions** - Click the ellipses button to open the **Edit Transitions** dialog box.



NOTE

If the workstep was previously linked, the destination workstep appears in the **Selected Transitions** list on the right.

5. Select the transition from the **Available Transitions** list, and then click **Add**. (Optionally, you can double-click any item in a list to move it to the opposite list.)



NOTE

When working with the **Transitions** property, keep the following in mind:

If you have multiple instances of a document in a workflow, and you want to mark this workstep complete without transitioning it, select **No Transition/Only Mark Workstep Complete**, and then click **Add**. This is useful in parallel workflows, where multiple worksteps must be completed before the document is transitioned. For example, if the same document has to be signed by several users before it transitions, this option would keep the worksteps from transitioning until they were all signed.

Select **Stop/Exit Workflow** to exit the workflow instance. In a parallel workflow, if any one instance of a document hits a **Stop/Exit Workflow** post-condition, all instances of that document will automatically exit the workflow.

Transition/Only Mark Workstep Complete, and **Stop/Exit Workflow** transitions cannot be combined with any other transitions.

6. After you have added or removed the needed transitions, click **OK**.
7. Under **Post-Condition Criteria**, specify the following properties.
 - **Document Signed** - To require that a document is signed before the post-condition is met, click the down arrow, and then select **True**.
 - **Tasks** - To require that tasks in the workstep are completed before the post-condition is met, click the ellipses button to open the **Task** dialog box, select the required tasks, and then click **OK**.

- **Workflow Instance Document** - To specify that a document exists before the post-condition is met, click the ellipses button to open the **Search Criteria** dialog box.
 1. In the index field boxes, type your search criteria that the document index values must meet.
 2. (Optional) In the **Search Type** box, click the down arrow, and then select the operator to apply to the search criteria.
 3. (Optional) Click **Test Criteria** to test the search criteria.
 4. (Optional) Click **Clear Criteria** to remove the search criteria.
 5. Click **OK** to save the search.

Verify Workflows

You can verify your complete workflow, including all pre-conditions, worksteps, tasks, and post-conditions for problems and errors. See "WorkFlow Verification Checks" on page 286, and "WorkFlow Verification Results" on the next page for a complete list of all verification checks, error messages.

To verify a workflow definition

1. If you have not already done so, open the **WorkFlow Designer**. (See "To open the WorkFlow Designer" on page 268 if you need instructions.)
2. On the left pane, select the workflow to validate.
3. On the **Home** ribbon, in the **Save** group, click **Verify Workflow** to open the **Workflow Verification** dialog box.
4. Click **Start** to begin the verification checks.
The results of each check appear in the **Status** column.
5. If any problems are found, click the link in the **Status** column to open the **Verification Results** dialog box. (See "WorkFlow Verification Checks" on page 286, and "WorkFlow Verification Results" on the next page for a complete list of all verification checks, warnings, and error messages.)
6. For the verification results, you have the following options:
 - To ignore the error or warning, select the check box in the **Ignore** column.
 - To clear all of the **Ignore** check boxes, click **Restore Ignored Tests**.
 - To remove the warnings from the **Verification Results** dialog box, select **Hide Warnings**.
7. After you have addressed errors and warnings, click **OK**.
8. (Optional) To save the verification results as a .txt file, click **Save Results**, specify a location and **File Name**, and then click **Save**.
9. Click **Finish** to close the **WorkFlow Verification** dialog box.

Workflow Verification Results

This table lists the verification results that can occur when you verify your workflow in the Workflow Designer. (See "Workflow Verification Checks" on page 286 for information about the checks that occur when you verify workflows.)

Type	Component	Description
WARNING	Worksteps (Automated)	The workstep "NAME" (ID: X) is part of an infinite loop.
WARNING	Worksteps (Automated)	The workstep "NAME" (ID: X) is not an initial workstep and no other worksteps transition to it.
WARNING	Worksteps (Automated)	The workstep "NAME" (ID: X) has one or more post-conditions with no tasks selected and no document search criteria defined. This configuration may result in unexpected behavior.
ERROR	Worksteps (Automated)	The workstep "NAME" (ID: X) has a post-condition "NAME" that has Workstep Completion configured and a task selected. If none of the post-conditions are met, the workstep will be transitioned to the Stop/Exit Workflow. This configuration may result in unexpected behavior.
ERROR	Worksteps (Custom Code)	The custom code workstep "CC Name" (ID: X) does not have a script defined.
ERROR	Worksteps (Custom Code)	The workstep "NAME" (ID: X) does not have a user assigned.
ERROR	Worksteps (Manual)	The workstep "NAME" (ID: X) has a owned/queued notification group set to a group (ID: X) that does not exist.
WARNING	Worksteps (Manual)	The workstep "NAME" (ID: X) does not have any post-conditions defined. This configuration may result in unexpected behavior.
ERROR	Worksteps (Manual)	The workstep "NAME" (ID: X) has its owned notification group set but the maximum time before notification is set to 0.
ERROR	Worksteps (Manual)	The workstep "NAME" (ID: X) has its queued notification group set but the maximum time before notification is set to 0.
ERROR	Worksteps (Manual)	The workstep "NAME" (ID: X) has its owned transition workstep set but the maximum time before transition is set to 0.
ERROR	Worksteps (Manual)	The workstep "NAME" (ID: X) has its queued transition workstep set but the maximum time before transition is set to 0.

Type	Component	Description
ERROR	Worksteps (Manual)	The workstep "NAME" (ID: X) does not have a user assigned.
WARNING	Parallel Workflows	The workflow branches from one to multiple instances, but never uses the Workstep Completion feature to consolidate back to one instance.
ERROR	Post-Conditions	The workstep "NAME" (ID: X) has a post-condition "NAME" (ID: X) that is searching the index field "NAME" which could not be found.
ERROR	Post-Conditions	The workstep "NAME" (ID: X) has a post-condition "NAME" (ID: X) that contains a Document Search (INDEX NAME = X) that is searching the index field "INDEX NAME" which could not be found.
ERROR	Pre-Conditions	The pre-condition "NAME" (ID: X) is searching the index field "NAME" which could not be found.
WARNING	Pre-Conditions	The pre-condition "NAME" (ID: X) does not have any search criteria defined, causing a wild card search to be used. This configuration may result in unexpected behavior.
ERROR	Tasks	The workstep "NAME" (ID: X) has a task "NAME" (ID: X) is set to change the index field "NAME" which could not be found.
WARNING	Tasks	The workstep "NAME" (ID: X) has a task "NAME" (ID: X) that has not been completely configured.
WARNING	Tasks	The workflow is set to inactive.
WARNING	Worksteps (Manual)	The workstep "NAME" (ID: X) is not an initial workstep and no other worksteps transition to it.
WARNING	Worksteps (Custom Code)	The workstep "NAME" (ID: X) is not an initial workstep and no other worksteps transition to it.

Workflow Verification Checks

This table lists the verification checks that occur when you verify your workflow in the Workflow Designer. (See "Workflow Verification Results" on page 284 for information about the results returned when you verify workflows.)

Test Group	Verification Check
Manual Worksteps	Manual worksteps not assigned to a user
Parallel Workflows	Parallel workflows that do not have a post-condition with Workstep Completion defined
Post-Conditions	Workflow Instance Document search criteria defined to fields that no longer exist
Post-Conditions	Document Package with fields defined that no longer exist
Pre-Conditions	New pre-conditions with no search criteria defined
Pre-Conditions	Pre-conditions that have search criteria defined to fields that no longer exist
Tasks	Force Index Value tasks set to change an index field that no longer exists
Tasks	Launch Application/Shell, Raise COM Event, Send Email, or Force Index Value tasks without Task Type Settings defined
Workflows	Workflow set to inactive
All Worksteps	Worksteps that are not initial worksteps and have no other worksteps with post-conditions transitioning to them – abandoned nodes
Automated Workstep	Automated workstep that transitions to itself without criteria defined
Automated Worksteps	Automated worksteps with no required tasks or search criteria in any post-condition
Automated Worksteps	Automated worksteps with a post-condition that has both a task selected and Workstep Completion configured
Custom Code Worksteps	Custom code worksteps not assigned to a user
Custom Code Worksteps	Custom code worksteps that do not have a script assigned
Manual Worksteps	Manual worksteps assigned to a notification group that no longer exists
Manual Worksteps	Manual worksteps with a time limit transition workstep that no longer exists
Manual Worksteps	Manual workstep with no post-condition defined
Manual Worksteps	Owned Notification Group set, but notification and transition times are not set

Test Group	Verification Check
Manual Worksteps	Queued Notification Group set, but notification and transition times are not set
Manual Workstep	Owned Transition Workstep set, but notification and transition times are not set
Manual Workstep	Queued Transition Workstep set, but notification and transition times are not set

Viewing Workflow Definition Diagrams

The left pane of the **WorkFlow Designer** lists the components of your workflow definition in alphabetical order. As your workflow definition becomes more complex, you might find it helpful to view the workflow definition as a diagram.

To view a workflow definition diagram

1. If you have not already done so, open the **WorkFlow Designer**. (See "To open the WorkFlow Designer" on page 268 if you need instructions.)
2. On the left pane, select the workflow to view.
3. (Optional) To view a diagram of the workflow definition without any viewing or editing options, on the **Home** ribbon, click **Designer**.



T I P

Anytime you are viewing the workflow diagram, you can reorganize the workflow by selecting a workstep, and then dragging it to another location. This will not change any links between worksteps.

4. Click the **Layout** ribbon to view a diagram of the workflow definition with the following options:
 - To zoom in on the diagram, click **Zoom In**.
 - To zoom out on the diagram, click **Zoom Out**.
 - To reset the zoom, Click **Reset Zoom**.
 - To fit the entire workflow diagram in the window, click **Fit To Size**.
 - To maximize the width of the diagram in the window, click **Scale to Width**.
 - To maximize the height of the diagram in the window, click **Scale to Height**.
 - To redraw the diagram so that no links cross, click **Redraw Workflow**, and then click **OK**.
 - See "Link Worksteps" on page 275 for information on linking worksteps.
 - To add shapes to your workflow diagram, click **Ellipse** or **Rectangle**, and then drag the shape to the location you want on the workflow diagram. You can then right-click the shape and do any of the following:
 - To add a workstep, click **Add Workstep**. (See "Add Worksteps " on page 272 for instructions.)
 - To delete the shape, click **Delete**.

- To change the color of the shape, click **Change Color**. Make your selections in the **Change Color** dialog box, and then click **OK**.

Activate and Deactivate a Workflow Definition

Deactivating a workflow definition stops any new workflow instances from being created. All existing workflow instances will continue to be processed.

To deactivate and activate a workflow definition

1. If you have not already done so, open the **WorkFlow Designer**. (See "To open the WorkFlow Designer" on page 268 if you need instructions.)
2. On the left pane, select the workflow to activate or deactivate.
3. On the right pane, under **Status**, click the **Active** property, and then do one of the following:
 - To activate the workflow definition, select **True**.
 - To deactivate the workflow definition, select **False**.

Configure Email Messages

You can create tasks in automated and manual worksteps that send email messages. (See "Add Tasks" on page 277 for instructions to add tasks to worksteps.) You can configure the sender, recipient, subject and components of the body of the message to populate with data from document indexes and the workflow instance.



NOTE

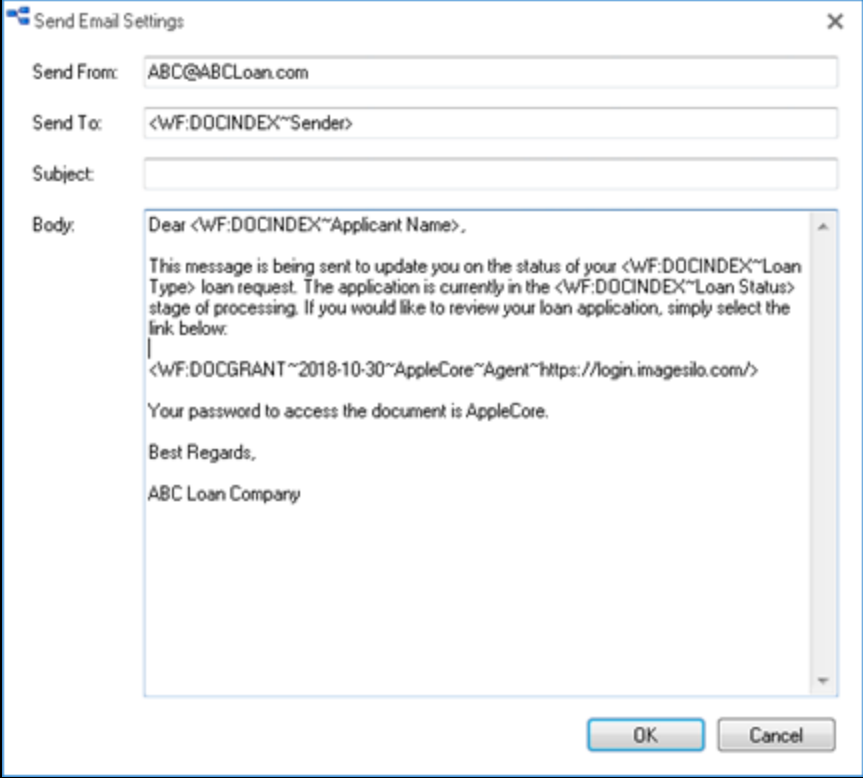
When an email message includes an E-Form, the E-Form is converted to a PDF file, and all fields are visible regardless of the assigned E-Form permissions.

To configure an email message

1. If you have not already done so, open the **WorkFlow Designer**. (See "To open the WorkFlow Designer" on page 268 if you need instructions.)
2. Add a task. (See "Add Tasks" on page 277 if you need instructions.)
3. On the right pane, under **Settings**, click the **Task Type** property.
4. Click the ellipses button, and then select **Send Email**.
5. Click the **Task Type Settings** property, and then click the ellipses button to open the **Send Email Settings** dialog box.
6. Configure the email message by typing the information you want to appear in the **Send From**, **Send To**, **Subject**, and **Body** boxes.
 - See "Email Message Tags" on page 290 for information about using email tags in these boxes.
 - See "CURRENTDATETIME Tags" on page 293 for information about using the CURRENTDATETIME tags to customize the email message.
7. Click **OK** to save the configuration.

E X A M P L E

If you use PaperVision Message Manager to capture incoming emails for a customer loan application project, you could set up a workflow to generate automated responses to applicants. You could configure the **Send Email Settings** dialog box using the following information:



Send Email Settings

Send From: ABC@ABCLoan.com

Send To: <WF:DOCINDEX~Sender>

Subject:

Body:

Dear <WF:DOCINDEX~Applicant Name>.

This message is being sent to update you on the status of your <WF:DOCINDEX~Loan Type> loan request. The application is currently in the <WF:DOCINDEX~Loan Status> stage of processing. If you would like to review your loan application, simply select the link below:

<WF:DOCGRANT~2018-10-30~AppleCore~Agent~https://login.imagesilo.com/>

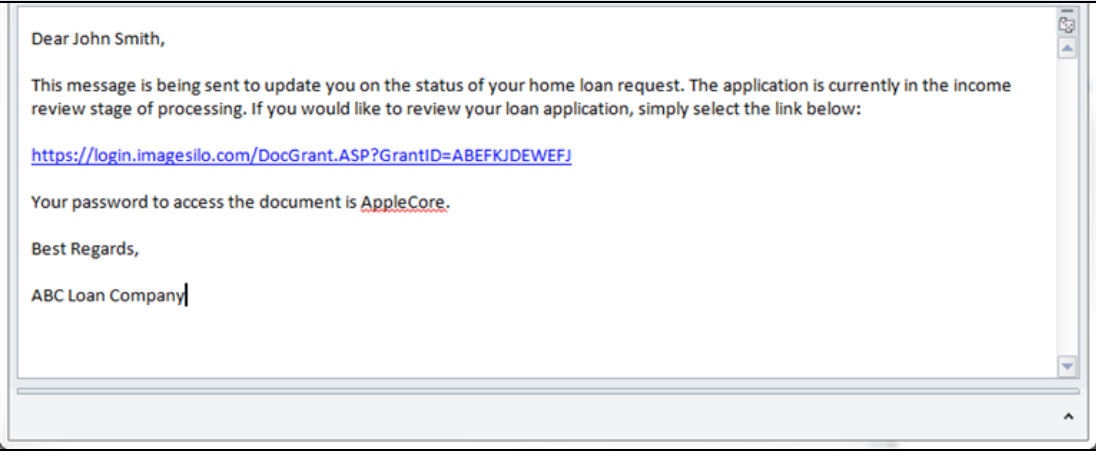
Your password to access the document is AppleCore.

Best Regards,

ABC Loan Company

OK Cancel

The resulting email message, based on the index values of the document, would produce an email message similar to the following:



Dear John Smith,

This message is being sent to update you on the status of your home loan request. The application is currently in the income review stage of processing. If you would like to review your loan application, simply select the link below:

<https://login.imagesilo.com/DocGrant.ASP?GrantID=ABEFKJDEWEFJ>

Your password to access the document is AppleCore.

Best Regards,


ABC Loan Company

Email Message Tags

You can use the following tags in the **Send Email Settings** dialog box, when you configure the **Task Type Settings** for the **Send Email** task. Except where indicated, tags can be used in any of the email values (send from, send to, subject, and body). All tag settings are required.

Tag	Description
<WF:ENTITYID>	Entity ID
<WF:WSINSTDOCID>	WorkFlow Instance Document ID
<WF:WFINSTID>	WorkFlow Instance ID
<WF:WSINSTID>	Workstep Instance ID
<WF:WFHISTORY>	WorkFlow Instance History
<WF:PROJID>	Project ID
<WF:WFDEFID>	WorkFlow Definition ID
<WF:WFNAME>	WorkFlow Definition Name
<WF:WSDEFID>	Workstep Definition ID
<WF:WSNAME>	Workstep Definition Name
<WF:CURRENTDATETIME>	Current Date/Time in "yyyy-mm-dd hh:nn:ss" format
<WF:DOCINDEX~FieldName>	Document index field value for the specified field (as specified by FieldName).
<WF:DOCGRANT~Expiration~Password~FieldsNotVisible~BaseURL>	<p>This tag creates a document grant with the specified expiration date/time (in "yyyy-mm-dd hh:nn:ss" format) and password (passwords cannot contain ~ or < symbols).</p> <p>FieldsNotVisible specifies the names of any index fields (pipe-delimited) that should not be visible in the document grant. BaseURL specifies the URL to the site where the document grant is created (for example, https://login.imagesilo.com). This tag is only valid in the email body. For a client (non-automated workstep) to be able to perform this, the user must have the security right to create document grants. Also, document security tracking for creating the grant is only performed if this is performed as a client operation.</p>

Tag	Description
<WF:LINKDOC~NewWin~BaseURL>	This tag creates a link (similar to document grants) that will force the user to log in. Once logged in, user will be taken directly to the document referenced by the workflow instance that generated the email. If NewWin is the number one (1), the document will be displayed in a new browser window. Otherwise the document will be displayed in the same window as the user login occurs. BaseURL specifies the URL to the site where the link is created (for example, https://login.imagesilo.com). This tag is only valid in the email body.
<WF:LINKWFINST~IgnoreLocateMsg~BaseURL>	This tag creates a link (similar to document grants) that will force the user to log in. Once logged in, user will be taken directly to the workflow instance that generated the email. If IgnoreLocateMsg is the number one (1), no message will be displayed in the event that the workstep is already owned (or couldn't be located), otherwise a message is displayed. BaseURL specifies the URL to the site where the link is created (for example, https://login.imagesilo.com). This tag is only valid in the email body.

Tag	Description
<WF:DOCPAGES~Format~x-y>	<p>Includes attachments of the specified page range (x-y). If the document consists of images, the images are converted into a single, multi-page TIF or PDF file (as specified by the Format value. Format and page range are required (otherwise an error occurs). Automated workflow email creation attaches the single PDF file (since all pages are within the single PDF), regardless of the specified page range. This tag is only valid in the email body.</p> <p>DataFlow/PVERM documents are converted to one of the following:</p> <ul style="list-style-type: none"> ■ A single text file (if no pages have overlays) ■ A single multi-page TIF or PDF file (if all pages have overlays) ■ A single text file (containing all of the pages of the document) AND a single TIF or PDF file (containing all of the pages that have overlays) if only some of the pages have overlays <hr/> <p> NOTE</p> <p>The temporary email attachment path must be specified by a global administrator. (See "To configure email settings" on page 58 for instructions.)</p> <hr/>

CURRENTDATETIME Tags

You can use the [CURRENTDATETIME] tag to populate values with the current date and time, or the current date and time with a specified offset. This is useful when you assign dates in workflow pre-conditions, create documents grants in an email task, and define date fields in automated worksteps when forcing an index value.

You can use the [CURRENTDATETIME] tag with an offset by specifying a number of years (Y), months (M), days (D), hours (H), minutes (N), or seconds (S). For example:

- [CURRENTDATETIME] = Current date and time
- [CURRENTDATETIME+1Y] = Current date and time + 1 year
- [CURRENTDATETIME - 6M] = Current date and time - 6 months
- [CURRENTDATETIME+2D] = Current date and time + 2 days
- [CURRENTDATETIME-96H] = Current date and time - 96 hours
- [CURRENTDATETIME+900M] = Current date and time + 900 minutes
- [CURRENTDATETIME+120S] = Current date and time + 120 seconds

This page was intentionally inserted without content.



CHAPTER 10

Reports

Report Functions	296
Report Archives	297
Document Access	299
Records Retention/Destruction	299
System Operations/Queries	301
Utilization	302
WorkFlow History	303
WorkFlow Status	304



Report Functions

Reports provide a way for you to perform detailed security audits, track user productivity and utilization, view the history of WorkFlows, manage the status of WorkFlows, and view records retention and destruction information.

This content covers basic functions that are available for all reports, such as applying filters, printing, and exporting data. See "Report Archives" on the facing page for information about archives and instructions to perform archive tasks.

For information about the contents of each report and functions that are report-specific, see the following:

- See "Document Access" on page 299 for information about this report.
- See "Records Retention/Destruction" on page 299 for information about this report.
- See "System Operations/Queries" on page 301 for information about this report.
- See "Utilization" on page 302 for information about this report.
- See "WorkFlow History" on page 303 for information about this report.
- See "WorkFlow Status" on page 304 for information about this report.

To access reports

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Reports**.
3. On the right pane, click the report.
4. Do one of the following:
 - Double-click the selected item.
 - On the **Action** menu, point to **All Tasks**, and then click **View Report Name**.
 - On the toolbar, click **View**.
 - Right-click the selected item, and then click **View Report Name**.



NOTE

By default, reports are limited to the first 1000 items. You can increase or decrease this limit by changing the **Max Items** value in the report view window.

To apply or remove a report filter



NOTE

Filtering is not available for Utilization reports, but you can apply a filter to all other reports. If you enter filter criteria for multiple items, only items that meet all of the criteria are located.

1. Open the report. (See "To access reports" above if you need instructions.)
2. On the toolbar, click **Filter Report**.

3. In the **Filter Report** dialog box, do one of the following:
 - To apply a filter, enter the filter criteria, and then click **OK**.
 - To remove a filter, click **Clear Filter**, and then click **OK**.

To refresh reports

1. Open the report. (See "To access reports" on the previous page if you need instructions.)
2. On the toolbar, click **Refresh View**.

To print reports



NOTE

Reports are printed exactly as they appear on the screen.

1. Open the report. (See "To access reports" on the previous page if you need instructions.)
2. On the toolbar, click **Print Entire Report**.
3. In the **Print** dialog box, select the print options, and then click **OK**.

To export report data to an XML file

1. Open the report. (See "To access reports" on the previous page if you need instructions.)
2. Select the item(s) to export (hold down the Ctrl key to select multiple items).
3. On the toolbar, click **Export Selection**.
4. In the **Export Report** dialog box, select the location where the export file will go.
5. In the **File name** box, type a name for the export file, and then click **Save**.

Report Archives

Report archives provide a simple way to free up database space, while maintaining data to be reviewed at a later time. When you archive a report, an XML document is created with all of the report data for the specified date range. Then, the archived report data is removed from the active system.



NOTE

Report archive functions are available for all reports, except for the Records Retention/Destruction report and the WorkFlow Status report, as these reports represent live data, not historical data.



CAUTION

You cannot archive the information that appears when you double-click an item in the WorkFlow History, as it is not part of the WorkFlow History report. Archived WorkFlow reports do not include workflow transition and task completion details as that would create massive archives.

This content describes report archives and the tasks related to them. See "Report Functions" on the previous page for basic functions that are available for all reports, such as applying filters, printing, and exporting data.

To view report archives

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Reports**.
3. On the right pane, click the report.
4. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Archives**.
 - On the toolbar, click **Archives**.
 - Right-click the selected item, and then click **Archives**.
5. In the **Report Name Archives** dialog box, select the archive, and then click **View**.

To archive reports



CAUTION

You cannot archive the information that appears when you double-click an item in the WorkFlow History as it is not part of the WorkFlow History report. Archived WorkFlow reports do not include workflow transition and task completion details as that would create massive archives.

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Reports**.
3. On the right pane, click the report.
4. Do one of the following:
 - Double-click the selected item.
 - On the **Action** menu, point to **All Tasks**, and then click **View Report Name**.
 - On the toolbar, click **View**.
 - Right-click the selected item, and then click **View Report Name**.
5. On the toolbar, click **Archive Range**.
6. In the **Archive Range** dialog box, type the date range to archive, and then click **OK**.
7. Click **Yes** to confirm the archive operation.

The specified items are archived, and the report is automatically regenerated to display the changes.

To restore report archives



NOTE

Restoring report archives places the information back into the database. This function is available only for Document Access and System Operations/Queries archives.

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Reports**.

3. On the right pane, click the report.
4. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **Archives**.
 - On the toolbar, click **Archives**.
 - Right-click the selected item, and then click **Archives**.
5. In the **Report Name Archives** dialog box, select the archive(s) to restore (hold down the Ctrl key to select multiple items), and then click **Restore**.
6. Click **Yes** to confirm the restore operation.

Document Access

Document access reports provide detailed records of all documents that are accessed and include the following information:

- Date and time the document was accessed
- Name of the user who accessed the document
- Type of operation performed on the document
- Project in which the operation was performed
- Index values of the document on which the operation was performed
- Page range on which the operation was performed
- Disclosure recipient (when using enhanced auditing)
- Disclosure reason (when using enhanced auditing)
- Disclosure notes (when using enhanced auditing)
- Source IP address or computer name from which the document was accessed

See "Report Functions" on page 296 for instructions to access this report and perform tasks that are available for all reports, such as applying filters, printing, and exporting data.

See "Report Archives" on page 297 for information about archives and instructions to perform archive tasks.

Records Retention/Destruction

Records Retention/Destruction reports provide information about the retention (lock) and destruction dates of documents within a project, and include the following information:

- Document ID
- Document Index Fields
- Retention/Lock Date
- Destruction Date

See "Report Functions" on page 296 for instructions to perform tasks that are available for all reports, such as applying filters, printing, and exporting data.



NOTE

Report archive functions are not available for the Records Retention/Destruction report, as this report represents live data, not historical data.

The following procedures are specific to the Records Retention/Destruction report.

To access the Records Retention/Destruction report

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Reports**.
3. On the right pane, click **Records Retention/Destruction**, and then, do one of the following:
 - Double-click the selected item.
 - On the **Action** menu, point to **All Tasks**, and then click **View Records Retention/Destruction Report**.
 - On the toolbar, click **View**.
 - Right-click the selected item, and then click **View Records Retention/Destruction Report**.
4. On the toolbar, click **Filter Report**, and then, from the **Project** list, select a project.
5. (Optional) In the **Destruction Date** and **Lock Date** boxes, you can specify a date range.
6. Click **OK** to display the report.



NOTE

By default, reports are limited to the first 1000 items. You can increase or decrease this limit by changing the **Max Items** value in the report view window.

To view document lock and destruction information

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Reports**.
3. On the right pane, click **Records Retention/Destruction**, and then, do one of the following:
 - Double-click the selected item.
 - On the **Action** menu, point to **All Tasks**, and then click **View Records Retention/Destruction Report**.
 - On the toolbar, click **View**.
 - Right-click the selected item, and then click **View Records Retention/Destruction Report**.
4. On the toolbar, click **Filter Report**, and then, from the **Project** list, select a project.
5. (Optional) In the **Destruction Date** and **Lock Date** boxes, you can specify a date range.
6. Click **OK** to display the report.

7. Select the document, and then do one of the following:

- Double-click the selected item.
- On the toolbar, click **Lock/Destruction Info**.

The lock and destruction information for the document, including who or what applied the date and any comments made during the date application appears.

To navigate through documents

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Reports**.
3. On the right pane, click **Records Retention/Destruction**.
4. Do one of the following:
 - Double-click the selected item.
 - On the **Action** menu, point to **All Tasks**, and then click **View Records Retention/Destruction Report**.
 - On the toolbar, click **View**.
 - Right-click the selected item, and then click **View Records Retention/Destruction Report**.
5. In the **Records Retention/Destruction** window, on the toolbar you can click **Next** or **Previous** to navigate through groups of documents.

System Operations/Queries

System Operations/Queries reports provide detailed records of all system operations that were performed (such as password changes, access to projects, and queries executed) and include the following information:

- Date and time the operation was performed
- Name of the user who performed the operation
- Type of operation performed
- Information pertaining to the operation, including the specific SQL query used to execute the search
- Destruction Date
- Source IP address or computer name from which the operation was performed

See "Report Functions" on page 296 for instructions to access this report and perform tasks that are available for all reports, such as applying filters, printing, and exporting data.

See "Report Archives" on page 297 for information about archives and instructions to perform archive tasks.

Utilization

Utilization reports provide summary totals for system usage and include the following information:

- Entity ID and name
- Date and time range of the report
- Date and time the report generated
- Number of current users
- Number of pages viewed, printed, and sent via email by each user (Whether this information is included is determined by how entity properties are set by a global administrator. See "To set utilization report options" on page 86 for instructions to set this feature.)
- Storage utilization summary that includes:
 - Current full-text database size (in MB and GB)
 - Current utilization (in MB and GB)
 - Average utilization (in MB and GB) over a series of samples that record the current amount of storage in use at a specified time as defined by a global administrator. (You can set this option by configuring the **Storage Utilization Snapshots** operation. See "Configure Automation Service Scheduling" on page 61 for instructions.)
 - Number of samples
- Backup processing utilization in MB
- WorkFlow processing utilization in total workstep instances completed on each day of the report period
- E-Form processing utilization in submitted forms
- Migration processing utilization that includes:
 - Total size migrated in MB
 - Total amount of time in hours
 - Total number of documents migrated
- Project utilization for each project that includes:
 - Project ID and name
 - Storage in bytes
 - Total number of documents and pages within each project (Whether this information is included is determined by how entity properties are set by a global administrator. See "To set utilization report options" on page 86 for instructions to set this feature.)



NOTE

You can view additional information by looking at the Utilization report in an XML format. To access this format, export the report or view the report archive. See "Report Functions" on page 296 and "Report Archives" on page 297 for instructions.

See "Report Functions" on page 296 for instructions to perform tasks that are available for all reports, such as applying filters, printing, and exporting data.

See "Report Archives" on page 297 for information about archives and instructions to perform archive tasks.

To access the Utilization report

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Reports**.
3. On the right pane, click **Utilization**, and then, do one of the following:
 - Double-click the selected item.
 - On the **Action** menu, point to **All Tasks**, and then click **View Utilization Report**.
 - On the toolbar, click **View**.
 - Right-click the selected item, and then click **View Utilization Report**.
4. In the **From Date/Time** and **To Date/Time** boxes, you can specify a date range or use the default value.
5. Click **OK** to display the report.



NOTE

By default, reports are limited to the first 1000 items. You can increase or decrease this limit by changing the **Max Items** value in the report view window.

WorkFlow History

WorkFlow history reports provide information about completed WorkFlow instances and the individual worksteps associated with them and include the following information:

- WorkFlow instance ID
- WorkFlow name
- WorkFlow instance start time
- WorkFlow instance end time
- Length of time it took the WorkFlow instance to be completed (in minutes)
- Workstep instance ID
- Workstep name
- Workstep instance start time
- Workstep instance end time
- Length of time it took the workstep instance to be completed (in minutes)
- Name of the owner who completed the workstep instance
- When a specific WorkFlow or Workstep is used as a filter value, the report also includes any available information pertaining to the document associated with each item in the report.
- Document ID

See "Report Functions" on page 296 for instructions to access this report and perform tasks that are available for all reports, such as applying filters, printing, and exporting data.

See "Report Archives" on page 297 for information about archives and instructions to perform archive tasks.



CAUTION

You cannot archive the information that appears when you double-click an item in the WorkFlow History, as it is not part of the WorkFlow History report. Archived WorkFlow reports do not include workflow transition and task completion details as that would create massive archives.

To view the WorkFlow history of a WorkFlow instance

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Reports**.
3. On the right pane, click **WorkFlow History**.
4. Do one of the following:
 - Double-click the selected item.
 - On the **Action** menu, point to **All Tasks**, and then click **View WorkFlow History Report**.
 - On the toolbar, click **View**.
 - Right-click the selected item, and then click **View WorkFlow History Report**.
5. Select the WorkFlow instance, and then do one of the following:
 - Double-click the selected item.
 - On the toolbar, click **WorkFlow History**.

WorkFlow Status

WorkFlow status reports provide information about the state of active WorkFlow instances. WorkFlow status reports include the following information:

- WorkFlow instance ID
- WorkFlow name
- WorkFlow instance start time
- Length of time the WorkFlow has been active/uncompleted (in minutes)
- Current workstep for the WorkFlow
- Current workstep instance start time
- Length of time the workstep instance has been active/uncompleted (in minutes)
- Owner of the current workstep instance
- When a specific WorkFlow or Workstep is used as a filter value, the report also includes any available information pertaining to the document associated with each item in the report.

See "Report Functions" on page 296 for instructions to access this report and perform tasks that are available for all reports, such as applying filters, printing, and exporting data.



NOTE

Report archive functions are not available for the WorkFlow Status report, as this report represents live data, not historical data.

To view the WorkFlow status of a WorkFlow instance

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Reports**.
3. On the right pane, click **WorkFlow Status**.
4. Do one of the following:
 - Double-click the selected item.
 - On the **Action** menu, point to **All Tasks**, and then click **View WorkFlow Status**.
 - On the toolbar, click **View**.
 - Right-click the selected item, and then click **View WorkFlow Status**.
5. Select the WorkFlow instance, and then do one of the following:
 - Double-click the selected item.
 - On the toolbar, click **WorkFlow History**.

Move WorkFlow Instances to a Specific Workstep

System and WorkFlow administrators can take an active WorkFlow instance and transition it to a specific workstep (regardless of the current state of the WorkFlow). If the owner of a workstep instance is no longer with a company, the administrator can move the WorkFlow instance back to the same (current) workstep as an unowned workstep, or move it to an entirely different workstep in the WorkFlow.

To move WorkFlow instances to a specific workstep

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then click **Reports**.
3. On the right pane, click **WorkFlow Status**.
4. Do one of the following:
 - Double-click the selected item.
 - On the **Action** menu, point to **All Tasks**, and then click **View WorkFlow Status**.
 - On the toolbar, click **View**.
 - Right-click the selected item, and then click **View WorkFlow Status**.

5. Select the WorkFlow instance(s) to move (hold down the Ctrl key to select multiple items).
6. On the toolbar, click **Move to Workstep**.
7. In the **Select Workstep** dialog box, select the workstep to receive the WorkFlow instance(s).
8. Click **Yes** to confirm the operation.

The current worksteps are marked as completed (administratively), and the new workstep instance is created.

APPENDIX A

System Architecture

SQL Server Express Edition	308
Web vs. Application Servers	308
Web Services	309
No IIS Sessions Required	309
Load Balancing	310
Automation Service and Servers	310
Database Scaling	311
File Replication	312
System Design Scenarios Overview	312
Security Features Overview	316



SQL Server Express Edition

SQL Server Express Edition is a scaled down version of Microsoft SQL Server. This product gives you access to the benefits of client-server computing and scalability without having to purchase Microsoft SQL Server. However, if you eventually decide to purchase Microsoft SQL Server, the database easily transfers over. SQL Server Express Edition is much more scalable than a system based on any file-based database (such as FoxPro or Access). Because you can install SQL Server Express Edition on any current Microsoft operating system, you can decide whether to dedicate a database server, use a PaperVision Enterprise workstation to also act as the database server for everyone or a group of users, or install a stand-alone workstation of PaperVision Enterprise (with SQL Server Express Edition serving only the workstation where it is installed).

- SQL Server Express Edition is a data engine built and based on core SQL Server technology, but there are some differences between it and Microsoft SQL Server. Some of the more notable differences are described below:
- SQL Server Express Edition, when used for PaperVision Enterprise, does NOT require any license purchases (for either the server or client access licenses).
- SQL Server Express Edition supports databases with a maximum size of 10 GB. Most PaperVision Enterprise users will be hard pressed to exceed this limit.
- SQL Server Express Edition supports only one processor (with support for multiple-core processors), up to 1 GB of RAM (used by SQL Express Edition itself), and supports 32-bit and 64-bit operating systems.
- SQL Server Express Edition has a governor that is designed to optimize its performance on the wide array of operating systems that can act as a database server. Based on our research, using an "average" workload, you should be able to run upwards of 100 PaperVision Enterprise concurrent users before having to consider an upgrade to Microsoft SQL Server. However, scalability is impacted and determined by your workload and the hardware and software configuration of the machine that is acting as a PaperVision Enterprise Database Server.

Digitech Systems, LLC supports SQL Server Express 2008 R2 or later.

Web vs. Application Servers

This section explains the difference between web servers and application servers.

- Web Servers provide an interface for browser-based users to access PaperVision Enterprise, whether that is over the Internet or the intranet. Web servers redirect all of their back-end processing to application servers.
- Application Servers offload the processing from web servers and client applications. Application servers perform database lookups, cache document files, and so on.
- Web/Application Servers are simply servers that perform the duties of both web and application servers.

Technically, the difference between a PaperVision Enterprise web server and application server is very little. Both servers use Microsoft's IIS to either serve web pages or handle web services traffic. However, a web server (as opposed to a web/application server or an application server) will redirect all of its processing to a second server (or group of servers) to perform the back-end functions.

Configuring a web server to use a separate application server is done by modifying the **PVDM.ini** file in the **C:\Program Files (x86)\Digitech Systems\Common Files** directory, and using the appropriate configuration files for the document search and file services.

See the following sections for instructions:

- "Set Up Process Redirection" on page 320
- "Process Redirection with the PaperVision Document Search Service" on page 321
- "Process Redirection with the PaperVision File Service" on page 326

Web Services

PaperVision Enterprise makes extensive use of its own web services to provide the following benefits:

- All traffic is handled using standard Hyper Text Transfer Protocol (HTTP) or Hyper Text Transfer Protocol Secure (HTTPS) communication. This includes communications between the web server and application servers (if process redirection is used) or client workstations and the web/application servers. Using HTTP or HTTPS provides the following advantages:
 - You can implement load balancing for second-tier application servers that are accessed by the web servers or the client workstations to provide additional scalability and reliability (if using a group of application servers).
 - Traffic can be fully secured using SSL to encrypt the data.
 - Traffic can, if desired, easily traverse a firewall, allowing you to place your web servers in your DMZ and place your application servers (which communicate with the databases and document stores) into a separate, secured network.
- Every time one computer communicates with another, a "round trip" is made. By grouping operations into a single communication, our web services minimize the number of round trips to greatly reduce the amount of network traffic.
- Our web service API provides the necessary functionality to integrate the client-server communications of PaperVision Enterprise. For example, a developer could integrate the document searching and retrieval capabilities of PaperVision Enterprise into an existing web application.

No IIS Sessions Required

Internet Information Services (IIS) is an extensible web server created by Microsoft. The web applications and web services of PaperVision Enterprise do not require the use of IIS sessions. Therefore, you can disable IIS sessions on your IIS server to take advantage of performance gains.

In place of IIS sessions, PaperVision Enterprise uses its own session architecture as follows:

1. When a user logs into PaperVision Enterprise, a session identifier (session ID) is created. The user's credentials and access (state information) are stored in the database referenced by this session ID. The session ID is encrypted and then returned to the user's computer.
2. Every time the user performs an operation, such as searching, the information pertaining to that search is passed to the server along with the user's encrypted session ID. Depending on the type of operation performed, the state information for the session might be updated.
3. When the user logs out of the system, this session ID and its state information are destroyed.

In addition to the significant improvement in performance for individual web and application servers (over using IIS sessions), the session architecture of PaperVision Enterprise allows a load-balanced system to disregard any need for persistence.

EXAMPLE

Tom logs into PaperVision Enterprise using web server A, runs a query using web server B, and then retrieves a document from web server C. Tom is not aware that he is using multiple servers and experiences fast response time. If any of the servers went down, Tom would not know because the load balancing would automatically redirect him to another server.

Because there is no session or state communication required between the web and application servers when you use the session architecture of PaperVision Enterprise, you can add more servers without increasing the overhead for the existing system. (See "Load Balancing" below for more information.)

Load Balancing

Load balancing allows an application to run on multiple servers that share the load, enhancing scalability and reliability. The scalability comes from the ability to run on multiple servers at the same time and share information amongst the servers. If a server gets bogged down, the other servers can take up the slack. The reliability comes from the ability of a user to hit a different server if one goes down (often without the user knowing they were redirected to another server).

PaperVision Enterprise servers (web and application) can sit behind load balancing servers with little, if any, configuration specific to PaperVision Enterprise. In addition, you can use PaperVision Enterprise with Microsoft Windows built-in Network Load Balancing (NLB).

Because of the unique way that PaperVision Enterprise handles its operations, it can scale to an unlimited number of servers. Each new server can incrementally add more processing power without reaching a point of diminishing returns (assuming the rest of your environment is designed properly, including network, storage, and so on).

Automation Service and Servers

The automation service automatically runs the operations you add to its schedule. (See "Configure Automation Service Scheduling" on page 61 for instructions.) After you configure the automation service, without requiring any user intervention, it can:

- Log users out of the system who have been idle for too long
- Remove expired document grants
- Run automated WorkFlow and workstep instances
- Process any workstep instances that have exceeded their maximum time restrictions
- Import data groups
- Delete data groups
- Take storage utilization snapshots
- Compress the full-text database

You can install the automation service on a single computer or on multiple computers. Each of the operations can be handled by multiple servers (for example, you can have multiple servers importing data groups or processing automated workstep instances).

In addition, running multiple automation service processes on a single computer is supported. In this scenario, each automation service process is specified in the `SERVERNAME_INSTANCE` format. Using this feature, you can schedule one or multiple automated operations per server or instance. You can modify the number of automation service processes that can run simultaneously through the **PaperVision Enterprise Configuration Utility**. (See "Configure Multiple Automation Service Processes" on page 28 for instructions.)

Database Scaling

Because PaperVision Enterprise has unlimited scalability and is a highly available system, efficient communications between components is paramount. See the following sections for strategies to address any potential communication bottlenecks between web servers and application servers.

- "Web vs. Application Servers" on page 308
- "Web Services" on page 309
- "No IIS Sessions Required" on page 309
- "Load Balancing" on the previous page

The next step to ensure maximum communication efficiency is to appropriately scale your database server to accommodate thousands (or even billions) of requests from simultaneous users. Adding machines or processors to a SQL cluster increases availability, but not scalability. To provide unlimited scalability, PaperVision Enterprise lets you place entities in separate physical databases that can be spread across separate servers. This feature accommodates the following database scaling options:

- Placing all of the entities in a single database on a single server
- Splitting entities across multiple databases on a single (or multiple) servers
- Placing each entity on its own database in its own database cluster

You perform administration from the Administration Console, and after you specify for the system to create the new entity in a different database, it keeps track of which entity is on which database and redirects the requests to the correct database. For end-user applications, PaperVision Enterprise automatically routes all database queries to the appropriate database server. The system handles the complexity of managing multiple databases so you don't have to.

File Replication

File replication capabilities are included as a core component of PaperVision Enterprise, and it can perform file replication on documents and full-text data in the system. This feature allows all changes to the document files and full-text databases to be replicated to another server and/or site for backup and high-availability applications. You can replicate your data to as many separate locations as necessary, either locally or across WAN connections to separate sites.

System Design Scenarios Overview

PaperVision Enterprise offers great flexibility with numerous options for system design. It can run on a single desktop computer or thousands of computers in distributed locations, and can reliably scale across multiple application servers, web servers, email servers and database servers. All of these servers can be leveraged, tiered and load-balanced to fit the needs of your site.

- See "Single User" below for a description of this design scenario.
- See "Workgroup" on the facing page for a description of this design scenario.
- See "Department" on page 314 for a description of this design scenario.
- See "Large Enterprise" on page 315 for a description of this design scenario.

Single User

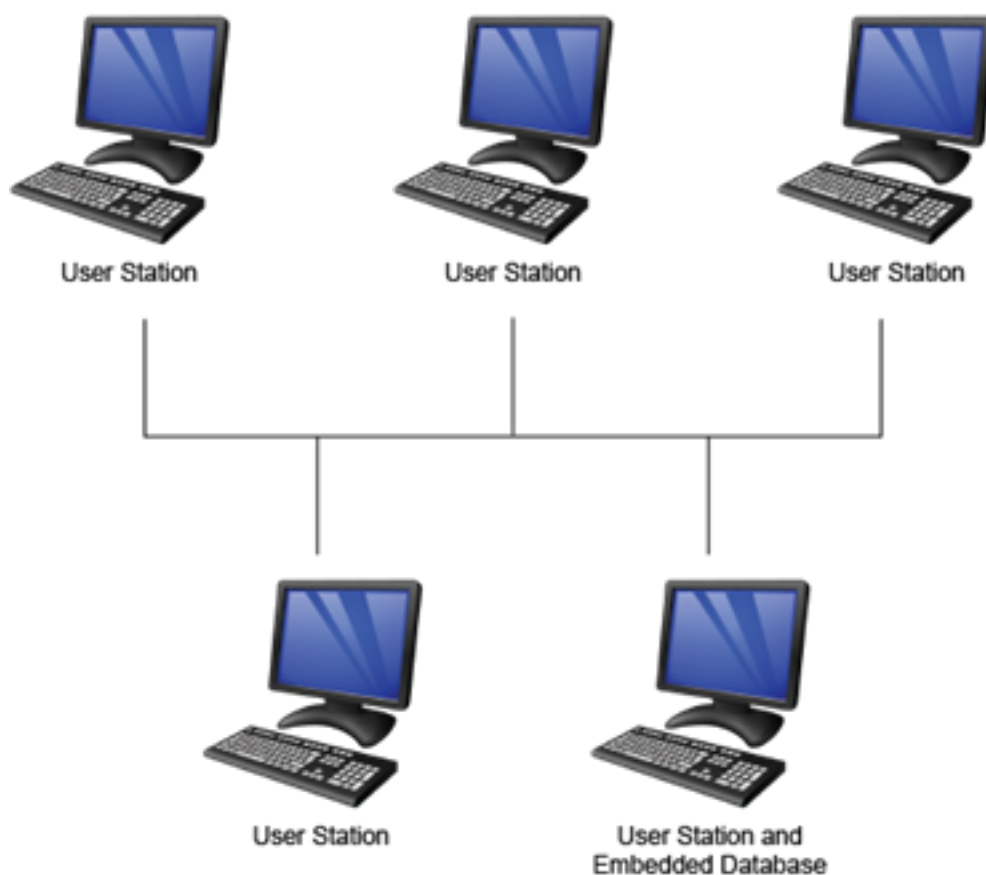
The single-user scenario occurs when only one work station needs access to PaperVision Enterprise. A network of any kind might not exist. In the single-user scenario, the one work station will house the SQL Server database, PaperVision Enterprise Administration Console, and PaperVision Enterprise Web Client.



Single User Station

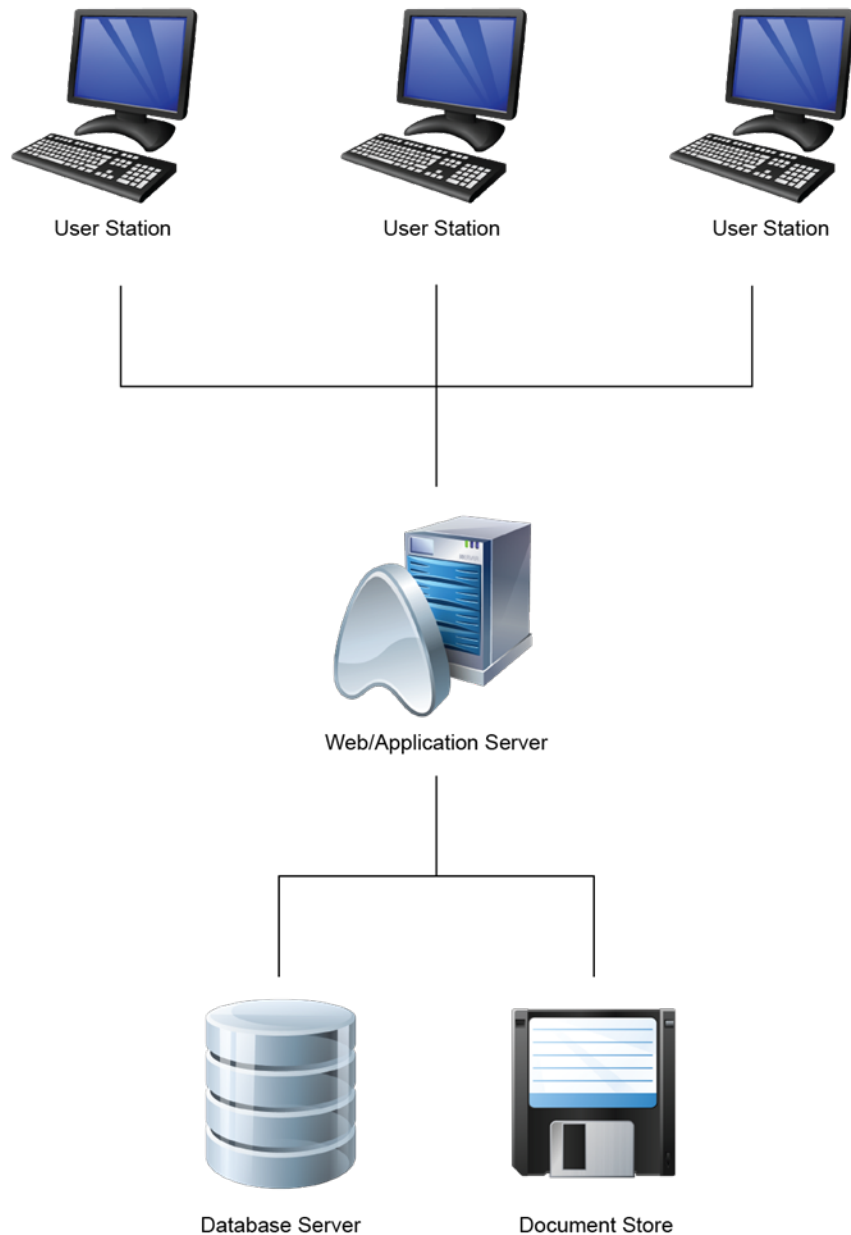
Workgroup

In a workgroup (up to 20 users), all of the clients access PaperVision Enterprise without a PaperVision server (other than a non-dedicated database). In a small workgroup, each system installs only PaperVision Enterprise, with the exception of a single workstation that also has the SQL Server database and Administration Console application installed. All of the other systems connect to the database workstation and interact directly with any document stores.



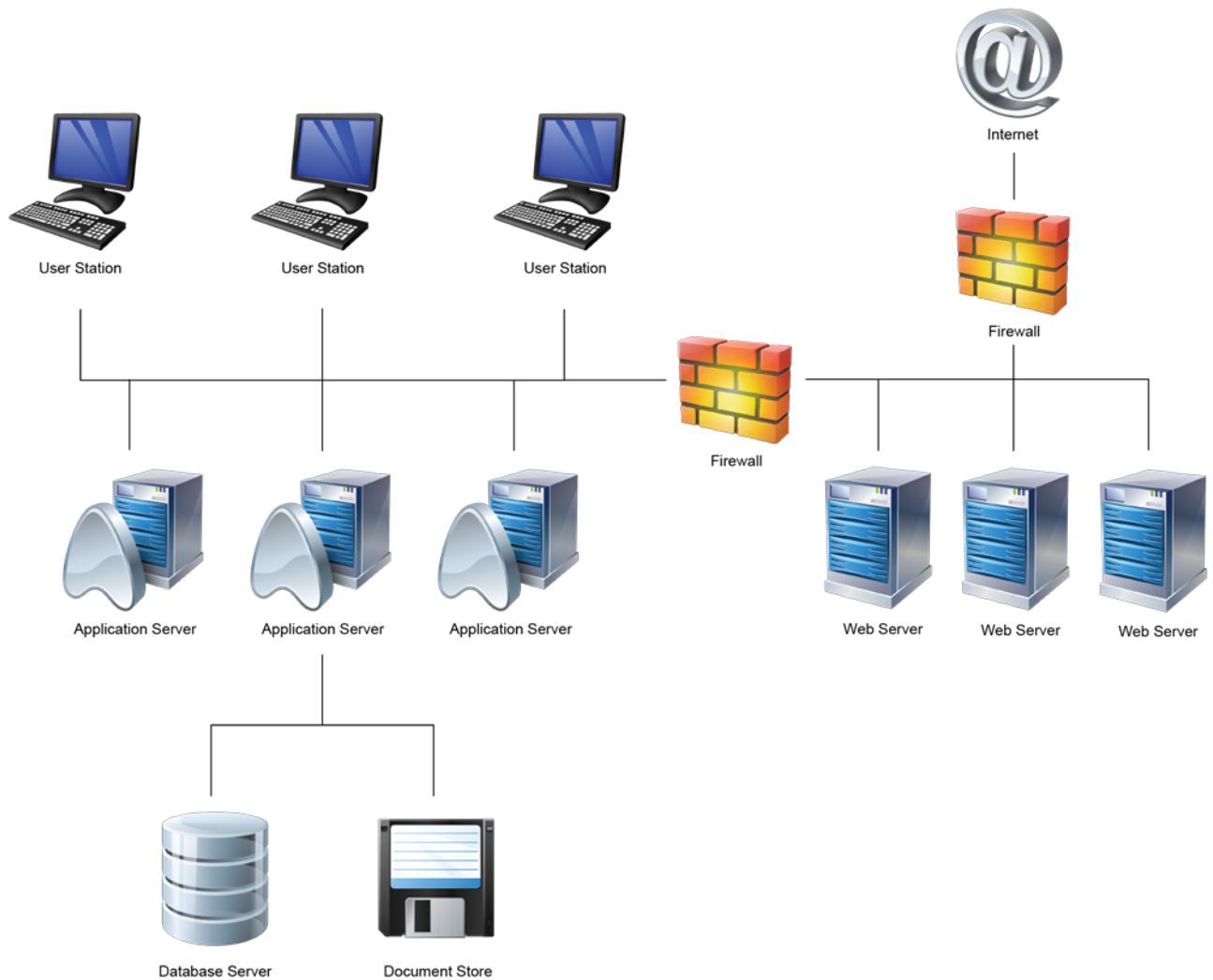
Department

In a department scenario (with hundreds of users), there might be users accessing the system via both ImageSilo and PaperVision Enterprise. For a departmental solution, we recommend that you seriously evaluate your need for Microsoft SQL Server (rather than using SQL Server 2008 R2 Express Edition) to meet your scalability needs. The user stations interact with the web/application server, and it handles all of the necessary transactions with the database server and the document store.



Large Enterprise

PaperVision Enterprise easily scales to handle the needs of an entire enterprise. In this example, there are internal users (on an internal network) that access either the application servers (via PaperVision Enterprise) or the web servers (via their web browsers). The web servers (assumed to be load-balanced) redirect all of their processing to the application servers (also assumed to be load balanced). The application servers are the only servers that interact directly with the database or document store. This configuration can provide unlimited scalability.



Security Features Overview

Whether your system is accessed directly or through a third-party system using PaperVision Enterprise APIs, great lengths were taken to ensure its security. Robust security features at multiple levels ensure that you can manage and retrieve your information securely. See the sections listed below to learn more.

- See "Session ID Encryption" below for more information about this feature.
- See "Support for SSL and Non-Standard Ports" below for more information about this feature.
- See "Function-Level Verification" below for more information about this feature.
- See "Session Source Persistence" below for more information about this feature.
- See "IP Address Limiting" on the facing page for more information about this feature.
- See "Automatic Session Termination" on the facing page for more information about this feature.
- See "Data Segregation" on the facing page for more information about this feature.
- See "Data Encryption" on the facing page for more information about this feature.

Session ID Encryption

Regardless of whether your site uses Secure Socket Layers (SSL) for your web and application servers, PaperVision Enterprise encrypts the session ID that is passed back and forth between the clients and servers. This ensures that a session ID cannot be guessed to "hijack" another user's session.

Support for SSL and Non-Standard Ports

PaperVision Enterprise provides support for Secure Socket Layers (SSL) and non-standard ports at both the web server and the application server levels. The use of SSL enables full encryption of all traffic (including documents) between the client applications and the servers (and, if desired, the web servers and the application servers). The ability to use non-standard ports allows administrators to host multiple web applications under a single IP address. It also allows an administrator to make the communication between certain segments (for example, between the web server and the application server) a little more obscure (although we never advocate security through obscurity).

Function-Level Verification

Every call made to PaperVision Enterprise that has anything to do with your account or information is verified for security access. This is even enforced at the lowest-level APIs that are included with PaperVision Enterprise. This ensures that a hacker could not write an application using the PaperVision APIs that could access your information.

Session Source Persistence

You can configure your system so that all session activity is required to originate from the source of the original login. If enabled, all session activity is required to originate from the source of the original log in. This ensures that user sessions cannot be taken over to gain unauthorized access to documents. When a user logs in, the IP address (or computer name) used to gain access is tracked, and each time information is requested, the system verifies that the request originated from that same IP address (or

computer name). If not, the request for information is denied, and a notification is sent to the system administrators. (See "To set general security options" on page 138 for instructions.)

IP Address Limiting

You can limit access to the system to specific IP addresses or address ranges. This is helpful to ensure that access can only occur from specific locations. (See "To set login restrictions" on page 141 for instructions to set this feature.)

Automatic Session Termination

Each time a user logs in to PaperVision Enterprise a session is started. Every time a user accesses the server, the system verifies that the session is still valid, performs the requested operation, and then records the date and time of the last activity. If a user session is idle for too long (as specified by the administrator), the session may be automatically terminated. Automatically terminating a session logs the user out of the system. This feature is useful for releasing licenses that are unnecessarily being used, for example, a user went to lunch without logging out, or the application was closed without the user logging out. Terminating idle sessions also helps keep your system secure. See "Current Sessions" on page 91 to learn about the settings that determine when user sessions are automatically terminated.

Data Segregation

PaperVision Enterprise provides effective data segregation by using databases. All of the data for one entity is kept separate from the data of a different entity. In a hosting environment, this is a key factor to ensure that one entity cannot access the data of another. The system manages the segregated data (that might exist in separate physical databases or even on separate physical servers) from a centralized Administration Console so that each entity does not have to be managed from its own instance of an application.

Data Encryption

PaperVision Enterprise provides data encryption services using the industry-standard AES-256 encryption algorithm. In your security policy, you can define encryption keys and pass phrases to apply data encryption. This ensures that unauthorized users can never access the raw data. See "Encryption Keys" on page 135 for instructions to configure data encryption.

This page was intentionally inserted without content.



APPENDIX B

Various Configuration Items

Set Up Process Redirection	320
Configure Document Search Service for SSL	329
Document Search Service Performance Counters	330
Configure File Service for SSL	330
Set Custom Font and Colors	331
Customization Options	331
PaperVision Enterprise APIs	332
PaperVision Enterprise Web and ASPX Pages	332



Set Up Process Redirection

In PaperVision Enterprise, you can use process redirection to redirect SQL and file operations from a web server to an application server. This configuration is ideal to store the data on your internal network and allow users from the Internet to access it from the PaperVision Enterprise web client. PaperVision Enterprise is specifically engineered to do this in the most secure manner. Because the internal application server is the one accessing the data and placing it in the cache location on the web server, the external web server never needs access to the data stores. This ensures that if the DMZ is ever compromised your data is not vulnerable. This configuration also works well for offloading the work that one server has to do on your internal network.

Setup Assumptions

The following assumptions are made ONLY if the configuration includes a web server in the DMZ and the application server is part of the internal network:

1. A firewall is installed.
 - HTTP (or HTTPS traffic) should be allowed to originate from the PaperVision Enterprise web server (in the DMZ network) to the PaperVision Enterprise application server (in the internal network).
 - HTTP (or HTTPS traffic) should be allowed to the PaperVision Enterprise web server (in the DMZ network) from the Internet.
 - Appropriate traffic is allowed to traverse the firewall to support Microsoft's domains and trusts (see related Microsoft KB articles later in this document).
2. The PaperVision Enterprise web server is part of a Windows domain in the DMZ.
3. The PaperVision Enterprise application server is part of a different Windows domain on the internal network.
4. A one-way trust exists between the internal domain and the DMZ domain.
 - Internal domain is trusted
 - DMZ domain is trusting
5. IIS is installed on both the PaperVision Enterprise web server (in the DMZ network) and the PaperVision Enterprise application server (in the internal network).

For more information about domains and trusts, see the following links:

[Understanding Trust Transitivity](#)

[How to Configure a Firewall for Domains and Trusts](#)

Configuring a Web Server to Use a Separate Application Server



IMPORTANT

Complete the following configuration only after installing and configuring the product.

A web server can redirect only to an application server. Configuring a web server to use a separate application server is done by modifying the **PVDM.ini** file in the **C:\Program Files (x86)\Digitech Systems\Common Files** directory, and using the appropriate configuration files for the document search and file services. (See "Process Redirection with the PaperVision Document Search Service" below and "Process Redirection with the PaperVision File Service" on page 326 for instructions to configure these services.)

Insert the following two lines of text in the **PVDM.ini** file:

```
[PVDM]
REDIRECTREQ=http://yourappserverhere/
```

If your web server sits behind a load balancer, you should also add the following lines:

```
[PVDM-GLOBALSYSTEM]
WEBURL=http://yourwebserverhere/
```



NOTE

Alternatively, these URL addresses can contain the "https" protocol identifier.

Since the web server will never need to interact with the database, it is not necessary (nor recommended for security reasons) to start the PaperVision Administration Console and connect to a database on the web server.

Process Redirection with the PaperVision Document Search Service

The PaperVision Document Search Service is not configured for systems that are using process redirection or SSL by default. Therefore, you must use different **web.config** and **DocumentSearch.svc** files for the search service to work with these options. Which files you use depend on whether you are using SSL on the redirect server, and whether you are redirecting to a server using SSL. From the procedures that follow, use the one that describes your setup configuration to specify the correct preconfigured files. These procedures assume that PaperVision Enterprise is installed in the default directory (**C:\Program Files (x86)\Digitech Systems**).

To set up a web server not using SSL to redirect to a web/application server not using SSL

1. On the web server, in the **C:\Program Files (x86)\Digitech Systems\PaperVision\Services\DocumentSearch** folder, right-click the **DocumentSearch.svc** file, and then click **Rename**.

2. Rename the file to **DocumentSearch.svc.Default**.
3. Press Enter, and then click **Yes**.
4. Right-click the **DocumentSearch.svc.Redirect** file, and then click **Rename**.
5. Rename the file to **DocumentSearch.svc**.
6. Press Enter, and then click **Yes**.
7. Right-click the **web.config** file, and then click **Rename**.
8. Rename the file to **web.config.Default**.
9. Press Enter, and then click **Yes**.
10. Right-click the **web.config.HTTP_Redirect_HTTP** file, and then click **Rename**.
11. Rename the file to **web.config**.
12. Press Enter, and then click **Yes**.
13. Open the **web.config** file in Notepad.
14. Search for **http://**. (There is only one instance.)
15. Change the default URL to the URL to which you are redirecting.

For example, if you are redirecting to the server "ImageSilo," you would change the default URL from:

```
address-  
s=http://localhost:8081/Services/DocumentSearch/DocumentSearch.svc  
  
to  
  
address-  
s=http://ImageSilo/Services/DocumentSearch/DocumentSearch.svc
```

16. Click **Save**.
17. Restart IIS.

To set up a web server not using SSL to redirect to a web/application server using SSL

1. On the web server, in the **C:\Program Files (x86)\Digitech Systems\PaperVision\Services\DocumentSearch** folder, right-click the **DocumentSearch.svc** file, and then click **Rename**.
2. Rename the file to **DocumentSearch.svc.Default**.
3. Press Enter, and then click **Yes**.
4. Right-click the **DocumentSearch.svc.Redirect** file, and then click **Rename**.
5. Rename the file to **DocumentSearch.svc**.
6. Press Enter, and then click **Yes**.
7. Right-click the **web.config** file, and then click **Rename**.
8. Rename the file to **web.config.Default**.
9. Press Enter, and then click **Yes**.
10. Right-click the **web.config.HTTP_Redirect_SSL** file, and then click **Rename**.

11. Rename the file to **web.config**.
12. Press Enter, and then click **Yes**.
13. Open the **web.config** file in Notepad.
14. Search for **http://**. (There is only one instance.)
15. Change the default URL to the URL to which you are redirecting.

For example, if you are redirecting to the server "ImageSilo," you would change the default URL from:

```
address-
s=http://localhost:8081/Services/DocumentSearch/DocumentSearch.svc

to

address-
s=https://ImageSilo/Services/DocumentSearch/DocumentSearch.svc
```

16. Click **Save**.
17. Restart IIS.

To set up a web server using SSL to redirect to a web/application server not using SSL

1. On the web server, in the **C:\Program Files (x86)\Digitech Systems\PaperVision\Services\DocumentSearch** folder, right-click the **DocumentSearch.svc** file, and then click **Rename**.
2. Rename the file to **DocumentSearch.svc.Default**.
3. Press Enter, and then click **Yes**.
4. Right-click the **DocumentSearch.svc.Redirect** file, and then click **Rename**.
5. Rename the file to **DocumentSearch.svc**.
6. Press Enter, and then click **Yes**.
7. Right-click the **web.config** file, and then click **Rename**.
8. Rename the file to **web.config.Default**.
9. Press Enter, and then click **Yes**.
10. Right-click the **web.config.SSL_Redirect_HTTP** file, and then click **Rename**.
11. Rename the file to **web.config**.
12. Press Enter, and then click **Yes**.
13. Open the **web.config** file in Notepad.
14. Search for **http://**. (There is only one instance.)

15. Change the default URL to the URL to which you are redirecting.

For example, if you are redirecting to the server "ImageSilo," you would change the default URL from:

```
address-  
s=http://localhost:8081/Services/DocumentSearch/DocumentSearch.svc  
  
to  
  
address-  
s=http://ImageSilo/Services/DocumentSearch/DocumentSearch.svc
```

16. Click **Save**.
17. Restart IIS.

To set up a web server using SSL to redirect to a web/application server using SSL

1. On the web server, in the **C:\Program Files (x86)\Digitech Systems\PaperVision\Services\DocumentSearch** folder, right-click the **DocumentSearch.svc** file, and then click **Rename**.
2. Rename the file to **DocumentSearch.svc.Default**.
3. Press Enter, and then click **Yes**.
4. Right-click the **DocumentSearch.svc.Redirect** file, and then click **Rename**.
5. Rename the file to **DocumentSearch.svc**.
6. Press Enter, and then click **Yes**.
7. Right-click the **web.config** file, and then click **Rename**.
8. Rename the file to **web.config.Default**.
9. Press Enter, and then click **Yes**.
10. Right-click the **web.config.SSL_Redirect_SSL** file, and then click **Rename**.
11. Rename the file to **web.config**.
12. Press Enter, and then click **Yes**.
13. Open the **web.config** file in Notepad.
14. Search for **http://**. (There is only one instance.)

15. Change the default URL to the URL to which you are redirecting.

For example, if you are redirecting to the server "ImageSilo," you would change the default URL from:

```
address-
s=http://localhost:8081/Services/DocumentSearch/DocumentSearch.svc

to

address-
s=https://ImageSilo/Services/DocumentSearch/DocumentSearch.svc
```

16. Click **Save**.

17. Restart IIS.

To set up an application server at the end of a redirect



I M P O R T A N T

If the application server at the end of a redirect is not configured to use SSL, then no changes are required. If the application server is using SSL, then complete the following procedure.

1. On the application server, in the **C:\Program Files (x86)\Digitech Systems\PaperVision\Services\DocumentSearch** folder, right-click the **web.config** file, and then click **Rename**.
2. Rename the file to **web.config.Default**.
3. Press Enter, and then click **Yes**.
4. Right-click the **web.config.SSL** file, and then click **Rename**.
5. Rename the file to **web.config**.
6. Press Enter, and then click **Yes**.
7. Restart IIS.

Process Redirection with the PaperVision File Service

The PaperVision File Service is not configured for systems that are using process redirection or SSL by default. Therefore, you must use different **web.config** and **FileService.svc** files for the file service to work with these options. Which files you use depend on whether you are using SSL on the redirect server, and whether you are redirecting to a server using SSL. From the procedures that follow, use the one that describes your setup configuration to specify the correct preconfigured files. These procedures assume that PaperVision Enterprise is installed in the default directory (**C:\Program Files (x86)\Digitech Systems**).

To set up a web server not using SSL to redirect to a web/application server not using SSL

1. On the web server, in the **C:\Program Files (x86)\Digitech Systems\PaperVision\Services\FileService** folder, right-click the **FileService.svc** file, and then click **Rename**.
2. Rename the file to **FileService.svc.Default**.
3. Press Enter, and then click **Yes**.
4. Right-click the **FileService.svc.Redirect** file, and then click **Rename**.
5. Rename the file to **FileService.svc**.
6. Press Enter, and then click **Yes**.
7. Right-click the **web.config** file, and then click **Rename**.
8. Rename the file to **web.config.Default**.
9. Press Enter, and then click **Yes**.
10. Right-click the **web.config.HTTP_Redirect_HTTP** file, and then click **Rename**.
11. Rename the file to **web.config**.
12. Press Enter, and then click **Yes**.
13. Open the **web.config** file in Notepad.
14. Search for **http://**. (There is only one instance.)
15. Change the default URL to the URL to which you are redirecting.

For example, if you are redirecting to the server "ImageSilo," you would change the default URL from:

```
address=http://localhost:8081/Services/FileService/FileService.svc
```

to

```
address=http://ImageSilo/Services/FileService/FileService.svc
```

16. Click **Save**.
17. Restart IIS.

To set up a web server not using SSL to redirect to a web/application server using SSL

1. On the web server, in the **C:\Program Files (x86)\Digitech Systems\PaperVision\Services\FileService** folder, right-click the **FileService.svc** file, and then click **Rename**.
2. Rename the file to **FileService.svc.Default**.
3. Press Enter, and then click **Yes**.
4. Right-click the **FileService.svc.Redirect** file, and then click **Rename**.
5. Rename the file to **FileService.svc**.
6. Press Enter, and then click **Yes**.
7. Right-click the **web.config** file, and then click **Rename**.
8. Rename the file to **web.config.Default**.
9. Press Enter, and then click **Yes**.
10. Right-click the **web.config.HTTP_Redirect_SSL** file, and then click **Rename**.
11. Rename the file to **web.config**.
12. Press Enter, and then click **Yes**.
13. Open the **web.config** file in Notepad.
14. Search for **http://**. (There is only one instance.)
15. Change the default URL to the URL to which you are redirecting.

For example, if you are redirecting to the server "ImageSilo," you would change the default URL from:

```
address=http://localhost:8081/Services/FileService/FileService.svc
```

to

```
address=https://ImageSilo/Services/FileService/FileService.svc
```

16. Click **Save**.
17. Restart IIS.

To set up a web server using SSL to redirect to a web/application server not using SSL

1. On the web server, in the **C:\Program Files (x86)\Digitech Systems\PaperVision\Services\FileService** folder, right-click the **FileService.svc** file, and then click **Rename**.
2. Rename the file to **FileService.svc.Default**.
3. Press Enter, and then click **Yes**.
4. Right-click the **FileService.svc.Redirect** file, and then click **Rename**.
5. Rename the file to **FileService.svc**.
6. Press Enter, and then click **Yes**.
7. Right-click the **web.config** file, and then click **Rename**.
8. Rename the file to **web.config.Default**.

9. Press Enter, and then click **Yes**.
10. Right-click the **web.config.SSL_Redirect_HTTP** file, and then click **Rename**.
11. Rename the file to **web.config**.
12. Press Enter, and then click **Yes**.
13. Open the **web.config** file in Notepad.
14. Search for **http://**. (There is only one instance.)
15. Change the default URL to the URL to which you are redirecting.

For example, if you are redirecting to the server "ImageSilo," you would change the default URL from:

```
address=http://localhost:8081/Services/FileService/FileService.svc  
to  
address=http://ImageSilo/Services/FileService/FileService.svc
```

16. Click **Save**.
17. Restart IIS.

To set up a web server using SSL to redirect to a web/application server using SSL

1. On the web server, in the **C:\Program Files (x86)\Digitech Systems\PaperVision\Services\FileService** folder, right-click the **FileService.svc** file, and then click **Rename**.
2. Rename the file to **FileService.svc.Default**.
3. Press Enter, and then click **Yes**.
4. Right-click the **FileService.svc.Redirect** file, and then click **Rename**.
5. Rename the file to **FileService.svc**.
6. Press Enter, and then click **Yes**.
7. Right-click the **web.config** file, and then click **Rename**.
8. Rename the file to **web.config.Default**.
9. Press Enter, and then click **Yes**.
10. Right-click the **web.config.SSL_Redirect_SSL** file, and then click **Rename**.
11. Rename the file to **web.config**.
12. Press Enter, and then click **Yes**.
13. Open the **web.config** file in Notepad.
14. Search for **http://**. (There is only one instance.)

15. Change the default URL to the URL to which you are redirecting.

For example, if you are redirecting to the server "ImageSilo," you would change the default URL from:

```
address=http://localhost:8081/Services/FileService/FileService.svc
```

to

```
address=https://ImageSilo/Services/FileService/FileService.svc
```

16. Click **Save**.
17. Restart IIS.

To set up an application server at the end of a redirect



IMPORTANT

If the application server at the end of a redirect is not configured to use SSL, then no changes are required. If the application server is using SSL, then complete the following procedure.

1. On the application server, in the **C:\Program Files (x86)\Digitech Systems\PaperVision\Services\FileService** folder, right-click the **web.config** file, and then click **Rename**.
2. Rename the file to **web.config.Default**.
3. Press Enter, and then click **Yes**.
4. Right-click the **web.config.SSL** file, and then click **Rename**.
5. Rename the file to **web.config**.
6. Press Enter, and then click **Yes**.
7. Restart IIS.

Configure Document Search Service for SSL

The PaperVision Document Search Service is not configured for systems that are using SSL. Therefore, you must make changes to the **web.config** file for the Document Search Service to work with SSL. The necessary preconfigured files are located at **C:\Program Files (x86)\Digitech Systems\PaperVision\Services\DocumentSearch** on the server where you installed PaperVision Enterprise.

To use the PaperVision Document Search Service with SSL

1. On the application or web server, in the **C:\Program Files (x86)\Digitech Systems\PaperVision\Services\DocumentSearch** folder, right-click the **web.config** file, and then click **Rename**.
2. Rename the file to **web.config.Default**.
3. Press Enter, and then click **Yes**.
4. Right-click the **web.config.SSL** file, and then click **Rename**.

5. Rename the file to **web.config**.
6. Press Enter, and then click **Yes**.
7. Restart IIS.

Document Search Service Performance Counters

PaperVision Enterprise includes several Windows performance counters for the Document Search Service. You can view these counters in the Windows Performance Monitor in the PaperVision Document Search Service category. For each Windows process running the Document Search Service, the following counters are available:

- **Average Service Request Time** – Average time to complete a service request. Each request can span multiple project searches.
- **Average Project Search Time** – Average time to complete a project search.
- **Error Count** – Number of requests resulting in an error.
- **Ratio of Successful Requests** – Ratio of successful (non-error) requests to total requests.
- **Completed Requests** – Number of service requests completed.
- **Completed Project Searches** – Number of project searches completed.
- **Completed Database Queries** – Number of database queries completed.
- **Completed Full-Text Queries** – Number of full-text queries completed.

In addition, a Total counter is available that sums the values for all running Document Search Service processes.

Configure File Service for SSL

The PaperVision File Service is not configured for systems that are using SSL. Therefore, you must make changes to the **web.config** file for the File Service to work with SSL. The necessary preconfigured files are located at **C:\Program Files (x86)\Digitech Systems\PaperVision\Services\FileService** on the server where you installed PaperVision Enterprise.

To use the PaperVision File Service with SSL

1. On the application or web server, in the **C:\Program Files (x86)\Digitech Systems\PaperVision\Services\FileService** folder, right-click the **web.config** file, and then click **Rename**.
2. Rename the file to **web.config.Default**.
3. Press Enter, and then click **Yes**.
4. Right-click the **web.config.SSL** file, and then click **Rename**.
5. Rename the file to **web.config**.
6. Press Enter, and then click **Yes**.
7. Restart IIS.

Set Custom Font and Colors

You can modify the colors, fonts, and font sizes for the PaperVision Enterprise Web Client by modifying the following cascading style sheets.

- **Support_Files\default_style.css** - This style sheet contains the majority of the style sheet attributes for the entire application.



NOTE

The contents of the **Support_Files\Grid.css** (that contained the style sheet attributes for pages displaying a result grid) and the **Support_Files\dndDefault.css** files are now located in the **Support_Files\default_style.css** style sheet.

- **Support_Files\admin_style.css** - This style sheet contains the style sheet attributes specific to the administration pages.
- **Support_Files\printPreview.xsl** - This file contains the style sheet and formatting attributes used when printing a result grid.
- **Javascript\dojo\dsi\themes\tundra\tundra.css** – This file contains the style sheet and formatting of buttons, check boxes, date calendar controls, dialog boxes, and so on.

Customization Options

You can customize many attributes of your system by modifying the **App_GlobalResources/globalSettings.resx** file located in the **PVEWeb** directory. The XML-based **globalSettings.resx** file contains the attributes in the following table.

This attribute	Defines
gblAboutName	The product name to display in the About window (defaults to PaperVision ^{&reg;} Enterprise).
gblAllowOverrideShowEntID	Whether a user can override the gblLoginShowEntID setting, by setting a cookie. When set to false, users cannot configure whether the Entity ID is displayed (defaults to true).
gblAttachURL	The ServerRefURL property, which is used by the PaperVision Viewer for functions such as determining the URL presented for document grants (defaults to an empty string "").
gblLoginInfoHTML	Additional text (in HTML format) that displays in the login prompt below the login button (defaults to an empty string "").
gblLoginInfoLegendTitle	The header title of the legend that contains the gblLoginInfoHTML text if the gblLoginInfoHTML value is populated (defaults to an empty string "").
gblLoginShowEntID	The default setting that determines if the Entity ID will display in the application (defaults to false).

This attribute	Defines
gblMaintenanceMsg	An HTML-formatted maintenance message that will display to all users, rather than presenting a login prompt (defaults to an empty string "").
gblMaxUploadSize	The maximum number of bytes that a file upload can contain. This setting must be smaller than the MaxRequestLength parameter defined for IIS to be evaluated (defaults to an empty string "").
gblResultsShowFirstDoc	Whether the system will display the first document in the search results automatically (defaults to false).
gblSecondaryTM	The Secondary Trademark Information that displays on the About page (defaults to an empty string "").
gblSiteImage	An image to display in the top, left corner of the interface (defaults to an empty string ""). If none is specified, the gblSiteName value is displayed as text instead.
gblSiteName	The name of the product to display throughout the application (defaults to PaperVision^{®} Enterprise).
gblSLAHTML	The HTML-formatted Service Level Agreement (SLA) text that displays on the About page (defaults to an empty string "").
gblUseCompressedJSFiles	Whether to reference the compressed pveCommon.js file that improves the loading speed of the pages in the Web Client (defaults to false, so compressed files will not be referenced). When this attribute is enabled, the contents of the pveCommon.js file under the PVEWeb\Javascript\ folder will be compressed.

PaperVision Enterprise APIs

PaperVision Enterprise includes a number of APIs that provide a means to extend or integrate its functionality into third-party applications and to create customized solutions. Restrictions and the terms of use for APIs are specified in the PaperVision Enterprise End-User License Agreement (EULA) that you received with the product. For API documentation, open the **PaperVision_Enterprise_APIGuide.pdf** file located in the **C:\Program Files (x86)\Digitech Systems\PaperVision\Docs** directory.

PaperVision Enterprise Web and ASPX Pages

PaperVision Enterprise Web is comprised of a series of ASPX and ASP pages (ASP pages are kept for backwards compatibility). These provide significant insight into using the PaperVision Enterprise APIs in a web-server application or browser-based environment.

PVESearchURL.aspx Page

PaperVision Enterprise Web includes a page called **PVESearchURL.aspx** that allows for quick integration with third-party applications. Via a URL, this page accepts remote login requests, user credentials, project selection, and search queries. It also determines what to do with search results (view the results or view the first document). By default, if no search results are returned, the Add New Documents and Scan New operations are not available. To ensure these operations are available, even when no results are returned by the original query, you must include the `ResultsType=List` parameter in your URL. If the `ResultsType=Docs` parameter is used, the Add New Documents and Scan New operations will not be available if no results are returned.



TIP

To redirect requests coming to the **PVESearchURL.aspx** page to the PaperVision Authentication Gateway, insert the query parameter `searchURL=true` into the Default.ASPX URL. To view a list of optional PVESearchURL query parameters, append `/PVESearchURL.aspx?` to the end of your PaperVision URL address.

PVESystemHealth.ASPX Page

The **PVESystemHealth.ASPX** page can verify that:

- The web server is working correctly and properly executing ASPX scripts (always on).
- The primary system database is accessible by the web/application server (`CheckType=1`).
- All of the databases for all of the entities are writable by the web/application server (`CheckType=2`).
- A user-defined list of document stores is accessible by the server (`CheckType=4`).

When accessing the **PVESystemHealth.ASPX** page, you can pass the `CheckType` value to specify which checks it will perform. If no `CheckType` value is passed, all checks are performed. The `CheckType` value can contain multiple checks by using a binary – or operation.

`PVESystemHealth.ASPX?CheckType=7` performs all checks.

To define the list of document stores (directories), create a file called **CHECK.DIR** in the **C:\Program Files\Digitech Systems\Common Files** directory. Type the full path to the directory that you want to verify (one path per line). A sample **CHECK.DIR** file is shown below:

```
\\storage1\pvdmsstore\
\\storage2\pvdmsstore\
Z:\document storage directory
```

This page was intentionally inserted without content.



APPENDIX C

Remote Authentication

Remote Authentication Functional Overview	336
Remote Authentication Use Scenarios	336
Configure PaperVision Authentication Gateway Settings	338



Remote Authentication Functional Overview

PaperVision Enterprise includes remote authentication gateway capabilities that allow organizations to integrate Windows authentication/single sign-on in a secure manner, regardless of whether the PaperVision repository is located in the same Active Directory domain as the authenticated users. Additionally, it lets users access their repository both from within their Active Directory domain and external to that domain, when Windows authentication/single sign-on is unavailable.

The following steps describe how remote authentication works:

1. The user opens the web browser and points it to the installed “PaperVision Authentication Gateway” server’s website. This “PaperVision Authentication Gateway” IIS website installation must have the ability to authenticate the user against Active Directory.
2. The authentication gateway reads an encrypted configuration file which indicates the encryption key value that is used to encrypt the user’s credentials. By using the security context that IIS is running under, the gateway determines the user’s domain name and user name (that is, DOMAIN\USER). It then encrypts this as the PaperVision user name using the specified encryption key value.
3. The gateway then redirects the user’s browser to their standard PaperVision repository’s login page (locally within the same domain, or remotely), passing the encrypted login credentials.
4. The PaperVision login process automatically detects that remotely authenticated credentials have been passed. As such, it uses the entity security policy’s **Remote Authentication Gateway Encryption Key** value (the value is used, not the name) to decrypt the authenticated credentials. If the credentials were not encrypted with the specified encryption key value, they cannot be decrypted and the user will not be automatically authenticated to the repository. If the credentials are properly encrypted (and hence, can be decrypted), the user is automatically logged in.

It is the common **Remote Authentication Gateway Encryption Key** value between the authentication gateway and the PaperVision repository that ensures only authorized authentication gateways may pass credentials. It is important to note that PaperVision has no visibility into a user’s Active Directory password. As such, it is neither necessary nor recommended to maintain consistent passwords between PaperVision and Active Directory for a user.

Remote Authentication Use Scenarios

You can use PaperVision’s remote authentication gateway facilities in nearly any environment. Following are likely scenarios and their general installation steps.

PaperVision Repository within the Same Active Directory Domain

In this scenario, the PaperVision Enterprise server is installed as a member of the users’ Active Directory domain. Although the easiest way of accomplishing this is to use the AutoLogin.ASPX page that is installed in the WebServer directory, doing so requires using Authenticated Access in the website under which PaperVision Enterprise is running. The primary problem with this is that all

activities performed by the server (that is, database and file access) are performed using the user's Active Directory credentials. As such, each user must be given explicit security access to the document storage shares/locations and the database server. A much better way to handle this situation is to set up two different websites on the same computer (typically requiring an IP address for each site). This allows server activities to be performed under a single security context (when the primary website is hit), while still allowing the user's security context to be determined by the authentication gateway website. The general installation steps for configuring this scenario follow.

1. Install and configure the PaperVision Enterprise server as usual (including making the necessary IIS configuration settings) on a server located in the Active Directory domain. However, when installing PaperVision, perform a Custom installation and add the PaperVision Authentication Gateway feature.
2. Configure a second IIS website on this server for the PaperVision Authentication Gateway.
3. Using the PaperVision Administration Console, configure a new encryption key, and then select that encryption key in the entity security policy's **Remote Authentication Gateway Encryption – Key Name** setting (located on the **Authentication** tab).
4. Run and configure the PaperVision Gateway Settings application. (See "Configure PaperVision Authentication Gateway Settings" on the next page if you need instructions.)

ImageSilo or PaperVision Repository within a Different Active Directory Domain

In this scenario, the PaperVision server is installed in either a different Active Directory domain (or no domain at all) as the users' Active Directory domain (that is, the PaperVision web server is located in the DMZ which doesn't have a trust relationship with the organization's internal domain). The general installation steps for configuring this scenario follow.

1. On a server within the user's Active Directory domain, install only the PaperVision Authentication Gateway. This is accomplished by performing a Custom installation and selecting **ONLY** the PaperVision Authentication Gateway.
2. Configure an IIS website on this server for the PaperVision Authentication Gateway.
3. Using the PaperVision Administration Console, configure a new encryption key, and then select that encryption key in the entity security policy's **Remote Authentication Gateway Encryption – Key Name** setting (located on the **Authentication** tab).
4. Run and configure the PaperVision Gateway Settings application. (See "Configure PaperVision Authentication Gateway Settings" on the next page if you need instructions.)

Configure PaperVision Authentication Gateway Settings

After PaperVision Enterprise Server is successfully installed and configured, you must configure the PaperVision Authentication Gateway using the **PaperVision Gateway Settings** utility. This utility lets administrators enter the encryption key and other settings used by the authentication gateway, and saves them in an AES-256 bit encrypted file that is specific to the machine on which it was created. For security purposes, you cannot copy the created PVRemoteAuth.XML file from one machine to another – each machine must be used to create its own file. (Refer to "Remote Authentication Functional Overview" on page 336 for more information about the remote authentication gateway capabilities in PaperVision Enterprise.)

Before you can configure PaperVision Gateway settings, you must complete the following tasks in the PaperVision Enterprise administration console.

- Create a user with a user name that exactly matches the user name logged in to the machine.
- Create an encryption key.
- Assign the encryption key to the security policy for the applicable entity.

The following procedures will walk you through each task required to configure the PaperVision Authentication Gateway.

To log in to the PaperVision Enterprise Administration Console

1. Double-click the **PaperVision Admin Console** icon.
2. In the **Administration Login** dialog box, type your user name and password.
If this is your first time logging in, the user name and password are both **ADMIN**.
3. If you want to log on as a global administrator, select the **Global** check box.
If this is your first time logging in, select the **Global** check box.

To create a PaperVision Enterprise user

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **General Security**.
3. Click **System Users**, and then do one of the following to open the **New User** dialog box:
 - On the **Action** menu, point to **All Tasks**, and then click **New User**.
 - On the toolbar, click **New**.
 - Right-click on the right pane, and then select **New User**.

4. In the **New User** dialog box, in the **User Name** box, type the name that will be used to log in to the computer.

**NOTE**

This user name must exactly match the user name logged into the computer, including the domain name if necessary. For example, if the user logged into the computer is JSmith on the Accounting network domain, the user name you create would be Accounting\JSmith. To assist you in determining the user logged into the machine, the Authentication Gateway includes a DebugUser.ASPX page that helps administrators troubleshoot IIS authentication issues by displaying the authorized user credentials detected by IIS. To access the DebugUser.ASPX page, navigate to `http://Gatewayservername:portnumber/DebugUser.ASPX`

5. (Optional) In the **Full Name** box, type the user's full name.
6. (Optional) In the **Email Address** box, type the user's email address.
7. In the **Password** box, type the user's password.
8. In the **Confirm Password** box, type the user's password again to confirm it.

**NOTE**

We recommend that you never leave a password set to a blank value, as it can pose a security risk.

9. To force the user to change the password the next time they log in, select **User must change password at next login**.
10. To allow the user to change the password at any time, select **User can change password when desired**.
11. In the **User Type** area, select the appropriate user type. To create a regular user, clear all of the check boxes. You can specify the following user types.
 - **System Administrator** - When you select this check box, the user can configure all administrative settings for the entity and have access to all functionality in all projects for that entity.

**NOTE**

If you select **System Administrator**, the other user types are automatically assigned to the user.

- **Workflow Administrator** - When you select this check box, the user can configure WorkFlow definitions for any project, as well as view WorkFlow history and WorkFlow status reports. By default, WorkFlow administrators do not have access to documents or functions in any projects and must be granted access to those projects explicitly.
- **Capture Administrator** - This setting is not used in PaperVision Enterprise. When you select this check box, the user can configure jobs and job steps in PaperVision Capture.
- **E-Form Administrator** - When you select this check box, the user can create E-Forms in PaperVision Enterprise.

12. After you have defined the user, click **OK** to save it.

To create an encryption key

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **General Security**.
3. Click **Encryption Keys**.
4. Do one of the following:
 - On the **Action** menu, point to **All Tasks**, and then click **New Encryption Key**.
 - On the toolbar, click **New**.
 - Right-click the selected item, and then click **New Encryption Key**.
5. In the **Add Encryption Key** dialog box, in the **Key Name** box, type a name to identify the key.
6. From the **Key Type** list, select the type of encryption to use for the key.
7. In the **Pass Phrase** box, type a pass phrase for generating the encryption key.



I M P O R T A N T

The value you type in the **Pass Phrase** box is the value you will use for the **Encryption Key Value** setting in the **PaperVision Gateway Settings** utility.

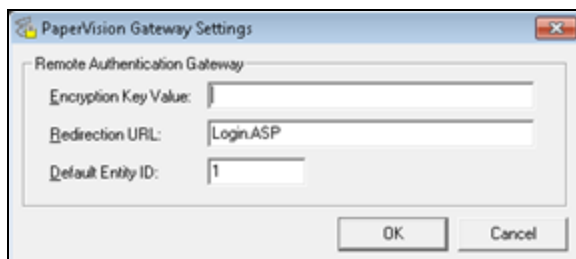
8. (Optional) In the **Description** box, you can type a description for the key. This is the only item that you can edit after the key is added.
9. Click **OK** to save the new encryption key.

To assign the encryption key to the entity security policy

1. After you have logged in to the Administration Console, on the left pane, expand **Entities**.
2. Expand the appropriate entity, and then expand **General Security**.
3. Right-click **Security Policy**, and then click **Configure Security Policy** to access the **Entity Security Policy** dialog box.
4. Click the **Authentication** tab, and then in the **Key Name** box, select the encryption key that you created.
5. Click **OK** to save the encryption key assignment.

To configure PaperVision Gateway Settings

1. On the taskbar in Windows, click the **Start** button, and then click **All Programs**.
2. Click the **Digitech Systems** folder, and then click **PaperVision Gateway Settings** to open the **PaperVision Gateway Settings** dialog box.



3. In the **Encryption Key Value** box, specify the pass phrase (not the encryption key name) which is identical to that created and selected in the entity security policy as the **Remote Authentication Gateway Encryption Key**.
4. In the **Redirection URL** box, specify the URL for the PaperVision Enterprise login page.
5. In the **Default Entity ID** box, specify the default entity ID to be used when logging in using the authentication gateway.

Accessing the Authentication Gateway

To access the Authentication Gateway

- Use your web browser to access the URL of your authentication gateway web site. The URL must include the server name where the Authentication Gateway is located and the applicable port number. For example, `http://Gatewayservername:portnumber`.

Using PaperVision Search URL to Access the Authentication Gateway

To log in using the PaperVision Authentication Gateway when running a PVESearchURL query, replace `/PVESearchURL.aspx?` with `?searchURL=true&`

Here is an example of what the URL might look like:

```
http://Gatewayservername:portnumber?searchURL=true&UserName=Public
&EntID=4&ProjID=1&IndexFields=Name&IndexValues=John Doe&ResultsType=list
```

To view a list of optional PVESearchURL query parameters using the PaperVision Authentication Gateway, you can access the following URL:

```
http://Gatewayservername:portnumber?searchURL=true
```

Using PaperVision Tools to Access the Authentication Gateway

PaperVision Enterprise Tools allows users to manage and upload documents directly from Microsoft® Word, Excel, PowerPoint and even Windows Explorer to PaperVision Enterprise. This tool makes it easy for users to engage in content management without leaving their Microsoft Office application. Drivers are also included to allow printing from any application that supports printing directly to PaperVision Enterprise.

To configure the Authentication Gateway in PaperVision Tools

1. After you have logged in to PaperVision Enterprise, click the down arrow next to your user name, and then click **Downloads**.
2. Locate **PaperVision Tools**, and then click **Download**.
3. When prompted, select whether you want to run or save the application.
4. If you saved the application, after the download is complete, run the executable file.

5. After the installation is complete, you can open Word, Excel, or PowerPoint, and then click the **Add-ins** ribbon to access the following dialog box where you can specify configuration options.



NOTE

When configuring the Authentication Gateway in PaperVision Tools, do not specify the web page name for either the Server URL (for example, Default.aspx) or Gateway URL (for example, Autologin.aspx).

The image shows a Windows-style dialog box titled "PaperVision Office Tool : Options". It has a "Help" button in the top-left corner. The dialog is divided into several sections. The "Connection" section has a radio button for "Use Internet Connection" which is selected, and a text box for "Server URL" containing "http://login.imagesilo.comt/". Below this is a checked checkbox for "Use Authentication Gateway" and a text box for "Gateway URL" containing "http://Gatewayservername.portnumber". The "Login Screen" section has an unchecked checkbox for "Display Entity ID". The "Add Documents Screen" section has a checked checkbox for "Remember Last Used Project" and an unchecked checkbox for "Logout After Adding Documents". The "PaperVision Enterprise Menu and/or Toolbar" section has a "Display:" dropdown menu set to "Both" and a "Button Style:" dropdown menu set to "Icon and Caption". At the bottom, there are three buttons: "Test Connection", "Save", and "Cancel".

6. In the **Server URL** box, type the URL to your PaperVision Enterprise log in page.
7. Select **Use Authentication Gateway**, and then type the URL to the authentication gateway site.
8. Click **Save**.

APPENDIX D

Search Assistance

Search Process Overview	344
Search Criteria Guidelines	346
Regular Expression Syntax and Metacharacters	348



Search Process Overview

Document searches are affected by options set from the Administration Console and options specified by users.

Global Administrators can set the following options:

- **Max. SQL database results per query** - This setting specifies the maximum number of documents returned for a search. If document grouping is enabled, fewer documents may be returned because some documents may be grouped to appear as one. (See "To set utilization limits" on page 51 for instructions.)
- **Max. Full-Text database results per query** - This setting specifies the maximum number of full-text search items returned by the full-text search engine. (See "To set utilization limits" on page 51 for instructions.)

Administrators can set the following option:

- **Document Grouping** - This setting specifies the default behavior for document grouping. It determines whether documents returned from searches are grouped, and if so, in what order. (See "To set the default document grouping" on page 84 for instructions.)

Users can set the following options as described in the *PaperVision Enterprise User Guide*:

- **Max. Results Per Query** - This setting specifies the maximum number of search results to appear on a search results page. This value cannot exceed the administrator-defined values described above.
- **Document Grouping** - This setting determines whether documents returned from searches are grouped, and if so, in what order. This user-defined value overrides the default behavior set by the administrator.



NOTE

When document grouping is selected, up to 100 documents with the same index values appear as if they were a single document.

The system follows the steps below when it searches for documents.

Search Process for Documents (Excluding Full-Text Search Criteria)

1. The index value query is run against the SQL database, the results are limited to the value specified by the **Max. Results Per Query** setting, and then sorted by the Document ID value.
2. Each document returned from that database query is checked to ensure that the requesting user has document-level access to it.
3. After removing documents, if there are fewer than the number specified by the **Max Results Per Query** setting, steps 1 and 2 are repeated for the next group of documents.

4. When the correct number of documents are found (or no more meet the criteria), the final set of documents are sorted based on the user's requested sort order and field.
5. The documents are queued and returned to the client. If document grouping is enabled, document index values are compared to determine if any document groups are created.

Search Process for Documents (Including Full-Text Search Criteria)

1. The full-text search criteria is submitted to the full-text database engine, and it returns, at most, the number of documents specified by the **Max. Full-Text database results per query** setting configured by the administrator. The engine returns the Document ID values (and additional information) of any documents that the full-text engine finds.
2. The submitted index value query (if any) is appended to require that the resulting documents have Document ID values that are in the list of those found by the full-text engine.
3. The submitted index value query is run against the SQL database, and the results are limited to the value specified by the **Max. Results Per Query** setting, and then the results are sorted by the Document ID value.
4. Each document returned from that database query is checked to ensure that the requesting user has document-level access to it.
5. After removing documents, if there are fewer than the number specified by the **Max Results Per Query** setting, steps 3 and 4 are repeated for the next group of documents.
6. When the correct number of documents are found (or no more meet the criteria), the final set of documents are sorted based on the user's requested sort order and field.
7. The documents are queued and returned to the client. Because a full-text search was run, no document grouping is used.

Search Criteria Guidelines

Flexible searching features enable fast and accurate document retrieval. To maximize your search results, use the search criteria guidelines described in the following tables.

To search for	Type	Example
Any number of unknown characters in an index value	*	T* returns any document where the selected index value begins with T *T* returns any document where the selected index value contains a T *T returns any document where the selected index value ends with T
A single unknown character in an index value	–	S_N returns SON, but will not return SOON _* returns any non-blank value
Multiple values within a single index field by using "and" and "or"	& = and ^ = or	*A*&*Z* returns all documents where the selected index value contains an A and a Z A^^Z* returns all documents where the selected index value begins with A or Z
Values in an index field that contain an ampersand	&&	Johnson && Johnson returns all documents where the selected index value is Johnson & Johnson
Documents of a specific age based on the current date and time.	[CURRENTDATETIME]+ or - the following: number of years Y number of months M number of days D number of hours H number of minutes N number of seconds S	[CURRENTDATETIME] = Current Date/Time [CURRENTDATETIME+1Y] = Current Date/Time plus 1 year [CURRENTDATETIME-12M] = Current Date/Time minus 12 months [CURRENTDATETIME+2D] = Current Date/Time plus 2 days [CURRENTDATETIME-96H] = Current Date/Time minus 96 hours [CURRENTDATETIME+900N] = Current Date/Time plus 900 minutes [CURRENTDATETIME+120S] = Current Date/Time plus 120 seconds
A range of dates	Beginning and ending dates in the format specified for the index value.	01/01/1995 , and 12/31/1999 returns all documents where the selected index value is between January 1, 1995, and December 31, 1999. Typing a single value instead of a range will return all documents with that index value.
A range of numbers or currency values.	Beginning and ending values.	100 , and 1000 returns all documents where the selected index value is between 100, and 1000. Typing a single value instead of a range, will return all documents with that index value.

The following table describes the valid search operators for full-text searches.

Search Operator	Description	Usage Example
AND	Specifies that both words must be present	apple AND pear Results in a search for documents that contain both "apple" and "pear"
OR	Specifies that at least one of the words must be present	apple OR pear Results in a search for documents that contain either "apple" or "pear"
NOT	Specifies that the word is not present; can be used with the AND and OR operators	apple AND NOT pear Results in a search for documents that contain "apple" and not "pear"
w/n	Specifies that words must occur no more than <i>n</i> words apart	apple w/6 pear Results in a search for documents that contain "apple" within six words of "pear"
*	A wildcard character that matches any number of letters	*apple AND pea* Results in a search for documents that contain any word that ends with "apple" and any word that begins with "pea"
?	A wildcard character that matches any single letter	apple AND pe?r Results in a search for documents that contain "apple" and any word that begins with "pe" and ends with "r" and contains one letter in between.

Regular Expression Syntax and Metacharacters

A regular expression is a pattern of text that consists of ordinary characters (for example, letters a through z) and special characters, known as metacharacters. The pattern describes one or more strings to match when searching a body of text. The regular expression serves as a template for matching a character pattern to the string being searched.

For more information about regular expressions, see the following links:

[Introduction to Regular Expressions](#)

[Regular Expression Syntax](#)

Some examples of how you can use regular expression syntax are shown below.

- **To locate:** Social Security Numbers such as: 123-12-1234
Use this syntax: `\d{3}-\d{2}-\d{4}`
- **To locate:** Blank lines
Use this syntax: `^\s*$`
- **To locate:** Various date formats such as 12.24.97, 12/24/97, and 12-24-97
Use this syntax: `((0?[1-9])|(1[012]))[- /.](0?[1-9]|[12][0-9]|3[01])[- /.](19|20)?[0-9]{2}`
- **To locate:** Days of the week in both Sunday and Sun formats
Use this syntax: `(Sun|Mon|(T(ues|hurs))|Fri)(day|.)?|Wed(.|nesday)?|Sat(.|urday)?|T((ue?)|(hu?r?)).?)`
- **To locate:** 16-digit credit card numbers
Use this syntax: `([0-9]{4}[-]?)^{4}`
- **To locate:** Any occurrence of SMITH followed by JONES (with or without characters between the two names)
Use this syntax: `SMITH.*JONES`

The following table contains a complete list of metacharacters and their behavior in the context of regular expressions:

Character	Description
\	Marks the next character as a special character, a literal, a back reference, or an octal escape. Example: 'n' matches the character "n". '\n' matches a newline character. The sequence '\\' matches "\" and \" matches "(".
^	Matches the position at the beginning of the input string.

Character	Description
\$	Matches the position at the end of the input string.
*	Matches the preceding character or subexpression zero or more times. Example: <code>zo*</code> matches "z" and "zoo". * is equivalent to <code>{0,}</code> .
+	Matches the preceding character or subexpression one or more times. Example: <code>zo+</code> matches "zo" and "zoo", but not "z". + is equivalent to <code>{1,}</code> .
?	Matches the preceding character or subexpression zero or one time. Example: <code>do(es)?</code> matches the "do" in "do" or "does". ? is equivalent to <code>{0,1}</code> .
<code>{n}</code>	<i>n</i> is a non-negative integer. Matches exactly <i>n</i> times. Example: <code>o{2}</code> does not match the 'o' in "Bob," but matches the two o's in "food."
<code>{n,}</code>	<i>n</i> is a non-negative integer. Matches at least <i>n</i> times. Example: <code>o{2,}</code> does not match the "o" in "Bob" and matches all the o's in "foooooo". <code>o{1,}</code> is equivalent to <code>o+</code> . <code>o{0,}</code> is equivalent to <code>o*</code> .
<code>{n,m}</code>	<i>m</i> and <i>n</i> are non-negative integers, where <i>n</i> ≤ <i>m</i> . Matches at least <i>n</i> and at most <i>m</i> times. Example: <code>o{1,3}</code> matches the first three o's in "foooooo". <code>o{0,1}</code> is equivalent to <code>o?</code> . Note: You cannot put a space between the comma and the numbers.
?	When this character immediately follows any of the other quantifiers (<code>*</code> , <code>+</code> , <code>?</code> , <code>{n}</code> , <code>{n,}</code> , <code>{n,m}</code>), the matching pattern is non-greedy. A non-greedy pattern matches as little of the searched string as possible, whereas the default greedy pattern matches as much of the searched string as possible. Example: In the string "oooo", <code>o+?</code> matches a single "o", while <code>o+</code> matches all 'o's.
.	Matches any single character except "\n". To match any character including the '\n', use a pattern such as <code>[s\S]</code> .
<code>(pattern)</code>	A subexpression that matches <i>pattern</i> and captures the match. The captured match can be retrieved from the resulting Matches collection using the \$0...\$9 properties. To match parentheses characters (), use <code>\(</code> or <code>\)</code> .
<code>(?:pattern)</code>	A subexpression that matches <i>pattern</i> but does not capture the match, that is, it is a non-capturing match that is not stored for possible later use. This is useful for combining parts of a pattern with the "or" character (<code> </code>). Example: <code>industr(?:y ies)</code> is a more economical expression than <code>industry industries</code> .

Character	Description
<code>(?=pattern)</code>	<p>A subexpression that performs a positive lookahead search, which matches the string at any point where a string matching <i>pattern</i> begins. This is a non-capturing match, that is, the match is not captured for possible later use.</p> <p>Example: 'Windows (=?95 98 NT 2000)' matches "Windows" in "Windows 2000" but not "Windows" in "Windows 3.1."</p> <p>Lookaheads do not consume characters, that is, after a match occurs, the search for the next match begins immediately following the last match, not after the characters that comprised the lookahead.</p>
<code>(?!pattern)</code>	<p>A subexpression that performs a negative lookahead search, which matches the search string at any point where a string not matching <i>pattern</i> begins. This is a non-capturing match, that is, the match is not captured for possible later use.</p> <p>Example: 'Windows (?!95 98 NT 2000)' matches "Windows" in "Windows 3.1" but does not match "Windows" in "Windows 2000."</p> <p>Lookaheads do not consume characters, that is, after a match occurs, the search for the next match begins immediately following the last match, not after the characters that comprised the lookahead.</p>
<code>x y</code>	<p>Matches either x or y.</p> <p>Example: 'z food' matches "z" or "food." '(z f)ood' matches "zood" or "food."</p>
<code>[xyz]</code>	<p>A character set. Matches any one of the enclosed characters.</p> <p>Example: '[abc]' matches the 'a' in "plain."</p>
<code>[^xyz]</code>	<p>A negative character set. Matches any character not enclosed.</p> <p>Example: '[^abc]' matches the 'p' in "plain."</p>
<code>[a-z]</code>	<p>A range of characters. Matches any character in the specified range.</p> <p>Example: '[a-z]' matches any lowercase alphabetic character in the range 'a' through 'z'.</p>
<code>[^a-z]</code>	<p>A negative range of characters. Matches any character not in the specified range.</p> <p>Example: '[^a-z]' matches any character not in the range 'a' through 'z'.</p>
<code>\b</code>	<p>Matches a word boundary, that is, the position between a word and a space.</p> <p>Example: 'er\b' matches the 'er' in "never" but not the 'er' in "verb."</p>
<code>\B</code>	<p>Matches a non-word boundary.</p> <p>Example: 'er\B' matches the 'er' in "verb" but not the 'er' in "never."</p>
<code>\cx</code>	<p>Matches the control character indicated by x.</p> <p>Example: \cM matches a Control-M or carriage return character. The value of x must be in the range of A-Z or a-z. If not, c is assumed to be a literal 'c' character.</p>
<code>\d</code>	<p>Matches a digit character. Equivalent to [0-9].</p>

Character	Description
\D	Matches a non-digit character. Equivalent to <code>[^0-9]</code> .
\f	Matches a form-feed character. Equivalent to <code>\x0c</code> and <code>\cL</code> .
\n	Matches a newline character. Equivalent to <code>\x0a</code> and <code>\cJ</code> .
\r	Matches a carriage-return character. Equivalent to <code>\x0d</code> and <code>\cM</code> .
\s	Matches any white space character including space, tab, form-feed, and so on. Equivalent to <code>[\f\n\r\t\v]</code> .
\S	Matches any non-white space character. Equivalent to <code>[^\f\n\r\t\v]</code> .
\t	Matches a tab character. Equivalent to <code>\x09</code> and <code>\cI</code> .
\v	Matches a vertical tab character. Equivalent to <code>\x0b</code> and <code>\cK</code> .
\w	Matches any word character including underscore. Equivalent to <code>'[A-Za-z0-9_]'</code> .
\W	Matches any nonword character. Equivalent to <code>'[^A-Za-z0-9_]'</code> .
\xn	Matches <i>n</i> , where <i>n</i> is a hexadecimal escape value. Hexadecimal escape values must be exactly two digits long. Example: <code>'\x41'</code> matches "A". <code>'\x041'</code> is equivalent to <code>'\x04'</code> & <code>'1'</code> . Allows ASCII codes to be used in regular expressions.
\num	Matches <i>num</i> , where <i>num</i> is a positive integer. A reference back to captured matches. Example: <code>'(.)1'</code> matches two consecutive identical characters.
\n	Identifies either an octal escape value or a backreference. If <code>\n</code> is preceded by at least <i>n</i> captured subexpressions, <i>n</i> is a backreference. Otherwise, <i>n</i> is an octal escape value if <i>n</i> is an octal digit (0-7).
\nm	Identifies either an octal escape value or a backreference. If <code>\nm</code> is preceded by at least <i>nm</i> captured subexpressions, <i>nm</i> is a backreference. If <code>\nm</code> is preceded by at least <i>n</i> captures, <i>n</i> is a backreference followed by literal <i>m</i> . If neither of the preceding conditions exists, <code>\nm</code> matches octal escape value <i>nm</i> when <i>n</i> and <i>m</i> are octal digits (0-7).
\nml	Matches octal escape value <i>nml</i> when <i>n</i> is an octal digit (0-3) and <i>m</i> and <i>l</i> are octal digits (0-7).
\un	Matches <i>n</i> , where <i>n</i> is a Unicode character expressed as four hexadecimal digits. Example: <code>\u00A9</code> matches the copyright symbol (©).

This page was intentionally inserted without content.



APPENDIX E

Utilities

PaperVision Enterprise Configuration Utility Overview	354
Digitech Logging Utility Overview	357



PaperVision Enterprise Configuration Utility Overview

After installation, if you need to reconfigure the PaperVision Automation Service, Client Server settings, or SQL Server connection information, you can use the PaperVision Enterprise Configuration Utility.

To open the PaperVision Enterprise Configuration Utility

1. On the applicable machine, start Windows.
2. On the taskbar, click the **Start** button, and then click **All Programs**.
3. Click the **Digitech Systems** folder, and then click **PaperVision Configuration Utility**.
4. If a **User Account Control** dialog box appears, click **Yes** to allow the configuration utility to make changes to the computer.
5. On the left pane, you can select the following options:
 - **Configure PaperVision Automation Service** - Click this option to change the number of simultaneous processes. (See "Change the Number of Simultaneous Processes" on the facing page for configuration instructions.)
 - **SQL Sever Connection Information** - Click this option to change the SQL server connection settings. (See "Change SQL Server Connection Information" on page 356 for configuration instructions.)

Change the Number of Simultaneous Processes

Your automation service processes were configured when the software was installed, but you can change the number of simultaneous processes through the **PaperVision Enterprise Configuration Utility**. You can configure multiple automation service processes to run on a single physical machine. In this scenario, each automation service process is specified in a `SERVERNAME_INSTANCE` format. The instance sequence starts with zero and increments by one for each added instance.

EXAMPLE

If your system had three simultaneous automation service processes configured on a machine named `SERVER`, the **Automation Service Status** listing would show the following under the **Automation Server** column.

`SERVER_0`

`SERVER_1`

`SERVER_2`

To change the number of simultaneous processes

1. Open the **PaperVision Enterprise Configuration Utility**. (See "To open the PaperVision Enterprise Configuration Utility" on the previous page if you need help.)
2. On the left pane, click **Configure PaperVision Automation Service**.
3. On the right pane, in the **Simultaneous Processes** box, specify the number of the simultaneous processes you want to use, and then click **Save**.
4. On the **Configure PaperVision Automation Service** dialog box, click **Yes** to restart the service. If you click **No**, you must manually restart the service. Your changes will not take effect until the service has been restarted.

Change SQL Server Connection Information

In the **PaperVision Enterprise Configuration Utility**, you can change the SQL server connection settings.

To change SQL server connection information

1. Open the **PaperVision Enterprise Configuration Utility**. (See "To open the PaperVision Enterprise Configuration Utility" on page 354 if you need help.)
2. On the left pane, click **SQL Server Connection Information**.
3. On the right pane, in the **Server IP/Name** box, type either the IP address or the machine name where the database resides.
4. In the **Database Name** box, type the database name that will be used to store data in PaperVision Enterprise.
5. In the **User Name** box, type the user name for the person who has the necessary permissions to create new users and add new data. If you do not want to use the System Administrator account, enter the name of a user that already exists and was granted the necessary permissions in SQL Server.
6. In the **Password** box, type the password associated with the user specified in the previous step. If you created a SQL user, type the password for that user.



NOTE

If you leave the **User Name** and **Password** fields blank, the database connection will use Windows Authentication credentials. Typing a user name and password for the database will supersede the Windows Authentication credentials.

7. In the **Confirm Password** box, type the password you specified to confirm it.
8. From the **Connection Type** list, select the connection type you want to use. If you select **TCP/IP**, then type the applicable port number in the **TCP/IP Port** box.
9. If the specified database name does not already exist, select **Create New Database**, and the new database will be automatically created in SQL Server.
10. If the specified user does not already exist, select **Create New User**. The new user will be automatically created in SQL Server and granted access to the database.



NOTE

If you select this option, a SQL Login prompt will appear. Type the user name and password for the account that has permission to create new users.

Digitech Logging Utility Overview

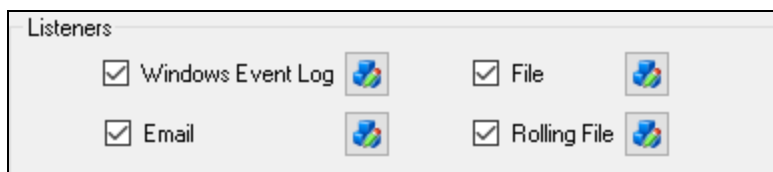
For your convenience, the Digitech Logging Utility is provided so that you can easily change some logging aspects without having to manually edit the XML configuration files. You can use the logging utility to modify configuration files for any Digitech Systems' product. The Digitech Logging Utility lets you specify:

- which configuration file to modify,
- the level of detail for the logs,
- where the log information is sent and/or stored,
- and the appearance of the content.

See "Configure the Digitech Logging Utility" on page 362 to specify configuration options.

Configure Listeners


After you complete the procedure under "To configure the Digitech Logging Utility" on page 362, you must specify where you want the log information to be sent and/or stored. You do this in the **Listeners** area in the **Digitech Logging Utility** dialog box.



The following procedures describe how to configure each type of listener.


To configure the Windows Event Log Listener

When you select **Windows Event Log**, it specifies that you want the log output to appear in the Windows **Event Viewer**. To access the **Event Viewer**, type **eventvwr** at the command prompt, and then press Enter.

1. If you haven't already done so, complete the procedure under "To configure the Digitech Logging Utility" on page 362.
2. In the **Listeners** area, select **Windows Event Log**, and then click  to open the **Windows Event Log Settings** dialog box.
3. In the **Source Name** box, type the name that you want to appear in the **Source** column of the **Event Viewer**, and then click **OK**.
4. If you are done configuring listeners, click **OK**. Otherwise, go to the instructions for the next listener you want to configure.

To configure the Email Listener


When you select **Email**, it specifies that you want the log output to be sent to an email address.

1. If you haven't already done so, complete the procedure under "To configure the Digitech Logging Utility" on page 362.
2. In the **Listeners** area, select **Email**, and then click  to open the **Email Settings** dialog box.
3. In the **SMTP Server** box, type the IP address or server name of the SMTP server.
4. In the **SMTP Port** box, type the applicable port number.
5. In the **To Address** box, type the email address to which the log information will be sent.
6. In the **From Address** box, type the email address from which the log information will be sent.
7. In the **Subject Line Starter (Optional)** box, type the subject you want to appear in the email notifications.
8. Click **OK**.
9. If you are done configuring listeners, click **OK**. Otherwise, go to the instructions for the next listener you want to configure.

To configure the File Listener

When you select **File**, it specifies that you want the log output to go to a file. So that you can easily locate the log file, you can specify the path and file name. The path you specify can contain any environment variable. The variable is resolved when the log is written. (To see a list of all the environment variables configured on your machine, go to a command prompt, type **set**, and then press Enter.)

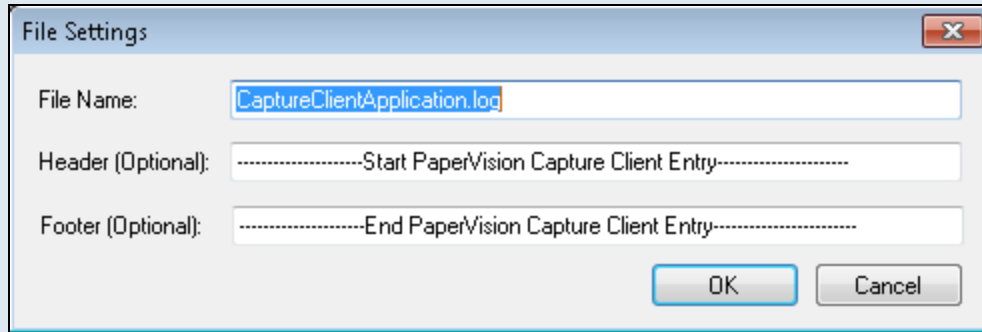
If you specify a directory with the file name, and that directory does not exist, the logging utility will create it. For example, if you type **C:\temp\logs\dsi.log** for the file name, the logging utility will create the **C:\temp\logs** directory if it does not already exist. When using the **File** option, log entries continue to accumulate in the same file which can cause the file to become very large. If you do not want to manually maintain this file, consider using the **Rolling File** option. (See "To configure the Rolling File Listener" on page 360 for more information.)

1. If you haven't already done so, complete the procedure under "To configure the Digitech Logging Utility" on page 362.
2. In the **Listeners** area, select **File**, and then click  to open the **File Settings** dialog box.
3. In the **File Name** box, type the path and/or file name for the log. If you do not include a path, the file you specify will be written to the Digitech installation directory.
4. (Optional) In the **Header** box, type a header that you want to appear at the beginning of each log entry in the file.
5. (Optional) In the **Footer** box, type a footer that you want to appear at the end of each log entry in the file.

6. Click **OK**.
7. If you are done configuring listeners, click **OK**. Otherwise, go to the instructions for the next listener you want to configure.

EXAMPLE

If your entries look like this,



then the log entry would appear similar to the following.


```
-----Start PaperVision Capture Client Entry-----
Timestamp: 4/7/2014 5:22:02 PM
Message: Accepting connections...
Category: Operational
EventId: 100
Severity: Information
Machine: BOBR-NOTEBOOK
OS Version: Microsoft Windows NT 6.1.7601 Service Pack 1
Application Domain: CaptureClient.exe
Process Id: 10932
Process Name: C:\dsi\bin\CaptureClient.exe
Win32 Thread Id 5332
Thread Name
-----End PaperVision Capture Client Entry-----
```

To configure the Rolling File Listener

When you select **Rolling File**, it specifies that you want the log output to go to a file, but to prevent the file from becoming too large, a new file is created based on the current date and time and the time interval that you specify. By default, the contents of a rolling file are abbreviated in comparison to the contents of a regular file.

So that you can easily locate the log file, you can specify the path and file name. The path you specify can contain any environment variable. The variable is resolved when the log is written. (To see a list of all the environment variables configured on your machine, go to a command prompt, type **set**, and then press Enter.) Additionally, if you specify a directory with the file name, and that directory does not exist, the logging utility will create it. For example, if you type **C:\temp\logs\dsi.log** for the file name, the logging utility will create the **C:\temp\logs** directory if it does not already exist.

The **Rolling File** option also supports the use of macros that are expanded when the file is written. Supported macros include: **{machineName}**, **{processID}**, **{timeStamp}**, or **{webSiteID}**.

1. If you haven't already done so, complete the procedure under "To configure the Digitech Logging Utility" on page 362.
2. In the **Listeners** area, select **Rolling File**, and then click  to open the **Rolling File Settings** dialog box.
3. In the **File Name** box, type the path and/or file name for the log. If you do not include a path, the file you specify is written to the Digitech installation directory. You can also include macros in this box.



N O T E

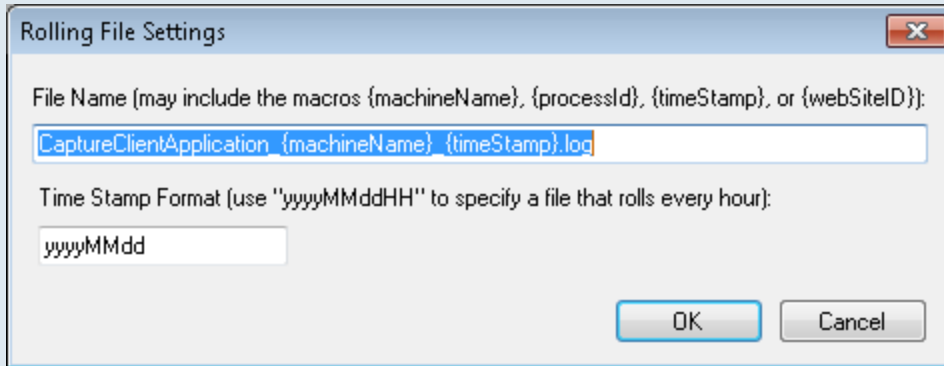
To specify a time interval for the creation of a new file, you must include the **{timeStamp}** macro in the **File Name** box.

4. In the **Time Stamp Format** box, specify the time interval for the creation of a new file. Use the **yyyyMMddHH** format, where **yyyy** equals the year, **MM** equals the month, **dd** equals the numerical day, and **HH** equals the hour in a 24-hour format. You control the interval by using only the portion of the format you want. For example, to create a new rolling log file on a daily basis, you would type **yyyyMMdd**. To create a new rolling log file on an hourly basis, type **yyyyMMddHH**.

5. Click **OK**.
6. If you are done configuring listeners, click **OK**. Otherwise, go to the instructions for the next listener you want to configure.

EXAMPLE

If your entries looked like this,



The output file would be **CaptureClientApplication_BOBR-NOTEBOOK_20140407.log**. The contents of a rolling file are abbreviated similar to the following sample

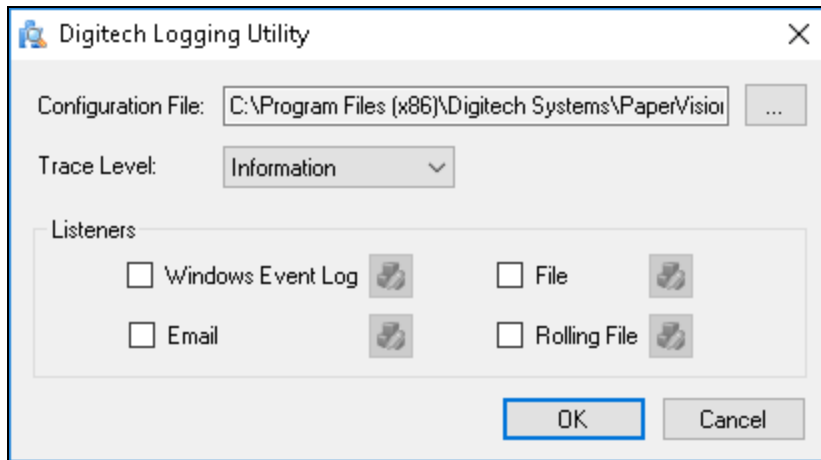
```
2014-04-07 17:31:23 Accepting connections...
2014-04-07 17:31:23 New incoming connection: 127.0.0.1
2014-04-07 17:31:23 Inside TryCheckSystemVersion_7_062413_
2014-04-07 17:31:23 Login user successfully with user name U and entityId 1
2014-04-07 17:31:23 Command from 127.0.0.1 processed successfully
2014-04-07 17:31:23 Client 127.0.0.1 disconnected (gracefully)
2014-04-07 17:31:23 Enabling manual .NET garbage collection every 300 seconds
2014-04-07 17:31:23 New incoming connection: 127.0.0.1
2014-04-07 17:31:23 Command from 127.0.0.1 processed successfully
2014-04-07 17:31:23 Client 127.0.0.1 disconnected (gracefully)
2014-04-07 17:31:23 New incoming connection: 127.0.0.1
2014-04-07 17:31:23 Command from 127.0.0.1 processed successfully
2014-04-07 17:31:23 Client 127.0.0.1 disconnected (gracefully)
2014-04-07 17:31:25 New incoming connection: 127.0.0.1
2014-04-07 17:31:26 Saved User ID 2 preferences
2014-04-07 17:31:26 Command from 127.0.0.1 processed successfully
2014-04-07 17:31:26 Client 127.0.0.1 disconnected (gracefully)
2014-04-07 17:31:26 New incoming connection: 127.0.0.1
2014-04-07 17:31:26 Command from 127.0.0.1 processed successfully
2014-04-07 17:31:26 Client 127.0.0.1 disconnected (gracefully)
```

Configure the Digitech Logging Utility

For all Digitech Systems software, logging settings are stored in the application's configuration file. If the executable file for your application were named **DigitechApp.exe**, then the name of the corresponding configuration file would be **DigitechApp.exe.config**, and it would be located in the same directory as the executable file. Configuration files are XML files that you can open and edit using any text editor, including Windows Notepad.

To configure the Digitech Logging Utility

1. Click **Start**, and then click **All Programs**.
2. Click the **Digitech Systems** folder, and then click **PaperVision Logging Utility** to open the **Digitech Logging Utility** dialog box.



3. Next to the **Configuration File** box, click the ellipsis button to open the **Select Config File** dialog box.
4. Click the **Look in** list to locate the directory where the configuration files are stored (typically, `Program Files\Digitech Systems\PaperVision`).
5. Click the configuration file for which you want to specify logging properties, and then click **Open**.
6. Click the **Trace Level** list, and then select one of the following options:
 - **Error** - This option specifies that recoverable errors are logged.
 - **Warning** - This option specifies that non-critical problems are logged.
 - **Information** - This option specifies that informational messages are logged.
 - **Verbose** - This option specifies that debugging trace information is logged.
 - **All** - This option specifies that all possible logging information is included.



NOTE

If you select **Verbose** or **All**, you are requesting the most possible output. These settings can generate a significant amount of output that requires extra processing which could slow application performance.

7. Go to "Configure Listeners" on page 357 to specify where you want the log information to be sent and/or stored.