

Peregrine

Get-Answers 4.1

Administration Guide

For Windows 2000, AIX, or Solaris

Copyright © 2003 Peregrine Systems, Inc. or its subsidiaries. All rights reserved.

Information contained in this document is proprietary to Peregrine Systems, Incorporated, and may be used or disclosed only with written permission from Peregrine Systems, Inc. This book, or any part thereof, may not be reproduced without the prior written permission of Peregrine Systems, Inc. This document refers to numerous products by their trade names. In most, if not all, cases these designations are claimed as Trademarks or Registered Trademarks by their respective companies.

Peregrine Systems® and ServiceCenter® are registered trademarks of Peregrine Systems, Inc. or its subsidiaries.

Microsoft, Windows, Windows NT, Windows 2000, and other names of Microsoft products referenced herein are trademarks or registered trademarks of Microsoft Corporation. Oracle is a registered trademark of Oracle Corporation. DB2 is a registered trademark of International Business Machines Corp.

This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>). This product also contains software developed by: Convera, Sun Microsystems, Inc., Netscape Communications Corporation, and InstallShield Software Corporation, RealObjects, Neva Object Technology, Inc., and NextPage Inc.

Portions of this documentation are provided by Convera Technologies, Inc. Copyright © 1998, 2002 by Convera Technologies, Inc. All rights reserved. Printed in the United States of America. The Convera(tm) name and design logo and the following are worldwide trademarks of Convera Technologies, Inc.: RetrievalWare®, RetrievalWare FileRoom(tm), Visual RetrievalWare(tm), and Screening Room®. All other names or marks may be registered trademarks or trademarks of their respective owners.

This document and the related software described in this manual are supplied under license or nondisclosure agreement and may be used or copied only in accordance with the terms of the agreement. The information in this document is subject to change without notice and does not represent a commitment on the part of Peregrine Systems, Inc. Contact Peregrine Systems, Inc., Customer Support to verify the date of the latest version of this document. The names of companies and individuals used in the sample database and in examples in the manuals are fictitious and are intended to illustrate the use of the software. Any resemblance to actual companies or individuals, whether past or present, is purely coincidental. If you need technical support for this product, or would like to request documentation for a product for which you are licensed, contact Peregrine Systems, Inc. Customer Support by email at support@peregrine.com. If you have comments or suggestions about this documentation, contact Peregrine Systems, Inc. Technical Publications by email at doc_comments@peregrine.com. This edition of the document applies to version 4.1 of the licensed program.

Peregrine Systems, Inc.
3611 Valley Centre Drive San Diego, CA 92130
Tel 800.638.5231 or 858.481.5000
Fax 858.481.1751
www.peregrine.com



Contents

	About this Guide	11
	Book audience	12
	Related documentation	12
	Associated applications	13
	Typographical conventions	13
	Special elements	13
	Organization of the guide	14
	Contacting customer support	15
	Peregrine CenterPoint Web site	15
	Need further assistance?	15
	Documentation Web site	15
	Education Services Web Site	16
Chapter 1	Architecture Overview	17
	Peregrine OAA Platform architecture	19
	Archway internal architecture	22
	Archway requests	23
	The Document Manager	25
Chapter 2	Setting-up Get-Answers	27
	Users and roles.	28
	Users.	28
	Setting System Maintenance passwords	29
	Setting Administration passwords	30
	Roles.	31

	Working with roles	32
	Managing users and roles	34
	Capability keywords	41
	Categories and document ownership teams.	45
	Document ownership teams	45
	Categories	46
	Managing categories and document ownership teams	47
	Working with categories	47
	Working with document ownership teams	55
	Configuring Spider (Web crawler) files	60
	Starting and stopping the Web crawler	60
	Automating the Spider processes	61
	Spider configuration files	62
	Firewall setup	79
	Clearing KMspider indexes	80
	Integrating Get-Answers with AssetCenter	81
	Using Crystal Reports with Get-Answers	82
Chapter 3	Using the Peregrine Portal	83
	Logging in to the Peregrine Portal.	84
	Using the Activity menu.	85
	Personalizing the Peregrine Portal	86
	Adding components	86
	Changing the layout	89
	Changing themes	91
	Displaying form information	92
Chapter 4	Customizing the Peregrine Portal	95
	Deploying the Classic theme variations	96
	Changing the default theme	97
	Changing the header graphic for all themes.	97
	Creating a custom theme	99
	Layers properties.	103
	Changing framesets.	104
	Translating Get-Answers	106
	Editing existing translation strings files	107

	Adding new translation strings files	107
Chapter 5	Personalization	111
	Personalization overview	112
	Forms and functions	112
	Personalization interface	113
	Personalization icons	115
	Supporting personalization	115
	Activating Personalization.	116
	Personalization tasks	118
	Adding fields to a form	118
	Configuring field attributes	120
	Changing the label of a field	121
	Changing a field to read-only	121
	Making a field required	122
	Changing the size and span of a field	122
	Removing fields from a form	122
	Moving Personalizations from a development to a production environment.	123
Chapter 6	Schemas	125
	Understanding Document Schema Definitions	126
	How to use schemas	127
	Schema extensions	128
	Sample schema	128
	When to use schema extensions	129
	Extending schema extensions in Get-Answers	129
	Editing the schema extension files.	131
	Adding a new field to the Available Fields list.	131
	Hiding an existing field from the Available Fields list	132
	Changing the label a field displays in the Available Fields list	133
	Changing the list of forms where a field is available or visible	133
	Changing the physical mapping of a field	134
	Schema Elements and Attributes	136
	<?xml>.	136
	<schema>	136
	<documents>	136

	<document>	137
	<attribute>	140
	Documents	143
Chapter 7	Get-Answers Administration	145
	Accessing the Peregrine Portal Admin module	146
	Using the Control Panel.	148
	Viewing the Deployed Versions.	149
	Viewing the Server Log	150
	Using the Settings page	150
	Setting parameters using the Admin module	151
	Verifying Script Status	153
	Displaying Message Queues	153
	Showing Queue Status	154
	Importing and exporting personalizations	155
	Viewing adapter transactions.	155
	Using the IBM Websphere Portal	156
	Displaying form information.	156
	Displaying form details	158
	User self-registration	159
	Changing passwords	160
	Logging and monitoring user sessions	160
	Understanding the usage.log file	160
Chapter 8	Get-Answers Security	163
	Password encoding methods	164
	User registration	165
	Enabling the E-mail adapter	165
	Troubleshooting the MailAdapter connection	166
	Authenticating users	166
	Default security configuration	167
	Custom JAAS configuration	168
	JAAS LoginModule control flags	170
	JAAS configuration options	173
	Example: Defining an LDAP custom configuration	177
	Standard Sun Microsystems JAAS configuration	177

	Command line options	178
	Integrated Windows Authentication.	178
	Setting up Integrated Windows Authentication	179
	Testing the settings.	187
	Integrating with single sign-on tools.	187
	Testing access to Get-Answers from a single sign-on tool.	189
	Contact-based authentication	190
	Creating an alternate login page	195
	Creating a login Web page.	195
	Specifying an alternate authentication method	197
Chapter 9	Customizing Get-Answers	199
	Understanding the search engine Stop Words list	200
	Stop Words list exceptions	200
	New and deleted Stop words.	201
	Modifying the Stop Words list	202
	Using search engine dictionaries	203
	Updating indexes for search engine dictionary changes	204
	Setting up custom dictionaries	205
	expand.wgt and semantic.db.	205
	Setting up the user dictionary folders	205
	Modifying expand.wgt	206
	Modifying semantic.db	207
	Setting up the search engine	208
	Creating cross references and indexes	210
	Re-starting and testing the Get-Answers search engine.	210
	Customizing edit-on Pro	212
	Browser Settings.	212
	Java security considerations	213
	Style sheets support	215
	Displaying unknown tags	219
	Online help in edit-on Pro	219
	Customizing the edit-on Pro spelling checker.	219
	Spelling checker properties	220
	Adding words to the spelling checker	225

Chapter 10	Get-Answers Workflows	229
	Defining workflow templates	230
	Creating a workflow template	230
	Creating a workflow template from another template	253
	Modifying a Workflow template	253
	Deleting a Workflow template	255
	Creating a Component template	257
	Using Workflow Administration	260
	Accessing the Administration function	260
	Monitoring process instances	261
	Updating a process instance	262
	Deleting a process instance	263
	Starting a new process instance	264
	Viewing the Event Queue	267
	Setting Up the Request List	268
	Uploading JavaScript Files	275
	Importing/Exporting Workflow Templates	280
	Using the Request List	282
	Accessing My Requests	282
	Viewing Request Details	282
	Initiating a New Request	284
	Viewing Overdue Requests	285
	Admin Settings for Workflow	286
Chapter 11	Importing Legacy Data	287
	Converting legacy data	288
	Overview	288
	For a single import	290
	Varieties of documents to import	290
	Externally created documents	291
	.XML documents with metadata	291
	.XML ‘authored’ documents	292
	Creating XML export files	293
	Creating the XML documents	294
	Changing field size in the database	298

	Adding fields for search engine indexing (import).	298
	Adding fields for search engine indexing.	299
	Converting Knowlix data	301
	Preparing for the conversion from Knowlix	301
	Running the migration from Knowlix.	302
	Importing your data to Get-Answers	303
	Managing migrated documents.	305
	Setting up permissions	305
	Using the extended fields in searching.	307
	Extending the database	308
	Creating input and edit forms	308
	Creating views.	310
	Removing like-named document types	311
	Creating schema extensions	312
	Using schema extensions to manually add new fields	312
Chapter 12	Document Types and Views	315
	Document Types.	315
	Document Views.	316
	Using document types to manage documents.	316
	Adding a view to a document type	317
	Adding a role to a document view	323
	Adding a new document type	324
	Adding an input and edit form.	326
	Glossary.	329
	Index.	337

About this Guide

Get-Answers is a Web-based, knowledge management application that enables you to capture and search on knowledge. Using Get-Answers, you can improve the quality and accuracy of the knowledge used by people in your company to get their jobs done and avoid calls to the help desk.

The *Administration Guide* explains concepts and provides step-by-step instructions for configuring and administering Get-Answers.

Get-Answers uses the Peregrine Open Application Architecture (OAA) Platform, a software platform that provides features and functions common to the Peregrine products Get-Answers, Get-Services, and Get-Resources. You can run one or all of these products on the 4.1 version of the Peregrine OAA Platform, but the platform is not sold apart from at least one of these products.

Book audience

The *Administration Guide* was written for Get-Answers administrators. To use this guide most effectively, you need to have knowledge of the following:

- Your organization's process for performing software installations and your responsibilities within that process
- Peregrine products that have been previously installed
- Your system architecture
- Your operating system user interface
- Configuring and maintaining local area networks (LANs)
- System administration tasks in your environment
- System administration tasks for associated back-end products

Related documentation

As you use Get-Answers, you can refer to this related documentation:

- *Get-Answers Release Notes* provides information about new features, corrected issues, and known issues. This is provided as a hard copy.
- *Get-Answers Installation Guide* provides information about installing Get-Answers and the Peregrine® Open Application Architecture (OAA) platform, the Get-Answers Search Engine, setting up your Web server and application servers, creating the Get-Answers database, and populating that database with sample data. This is provided as a hard copy.
- *Get-Answers User's Guide* which provides information about searching the Get-Answers document collection, working with documents, authoring new documents, and generating reports. This book is located on the Get-Answers CD.
- *Notification Services Quick Start Guide* explains concepts, provides step-by-step instructions, and describes tasks that you can complete in Notification Services. It also provides information on configuring and administering Notification Services. Notification services works with other Peregrine applications to enable users to send and receive notifications.

Associated applications

You can integrate Get-Answers with Peregrine's ServiceCenter. The *Get-Answers Installation Guide* describes how to do this. This guide does not contain information about products that may be used with Get-Answers, such as ServiceCenter. If you integrate Get-Answers with ServiceCenter, refer to the appropriate product documentation for information about using them with Get-Answers.

Note: If you are integrating Get-Answers with ServiceCenter, it must be installed and configured before you install Get-Answers.

Typographical conventions

This guide uses typeface conventions to indicate special terms and actions. These conventions and their meanings are:

Convention	Meaning
Sans serif	Information that you must type exactly as shown, code examples, output, and system messages appear in a sans serif font.
Bold	Button names, field names, menu names, and menu options appear in bold .
<i>Italics</i>	Variables and values that you must provide appear in <i>italics</i> . New terms also appear in <i>italics</i> .

Special elements

This book uses special elements to help you locate information. These special elements and their uses are shown in the following table:

Element	Usage
Important:	Information that is required to complete a task
Note:	Information that is of general interest

Element	Usage
Tip:	Information that can make a task easier or faster
Warning:	Information that is needed when there is a risk of losing data

Organization of the guide

The *Get-Answers Administration Guide* contains the following chapters.

- Chapter 1, *Architecture Overview*, describes the structure of the Peregrine OAA Platform, which Get-Answers uses.
- Chapter 2, *Setting-up Get-Answers*, provides information about managing Get-Answers document collections and users.
- Chapter 3, *Using the Peregrine Portal*, describes the Peregrine Portal, the interface that users see when they log in to Get-Answers.
- Chapter 4, *Customizing the Peregrine Portal*, tells you how to customize the look of the Peregrine Portal.
- Chapter 5, *Personalization*, shows you how to set up Get-Answers so that users can change the information on the forms they see within the application.
- Chapter 6, *Schemas*, describes document schema definitions and explains how they map data between Get-Answers and the database.
- Chapter 7, *Get-Answers Administration*, provides an overview of the Get-Answers Admin module.
- Chapter 8, *Get-Answers Security*, provides information about granting and protecting access to Get-Answers.
- Chapter 9, *Customizing Get-Answers*, provides information about modifying the stop word list, creating custom dictionaries, and customizing the spelling checker used with the RTF editor.
- Chapter 10, *Get-Answers Workflows*, provides information about workflows in general and the Triage and Editing workflows specifically.
- Chapter 11, *Document Types and Views*, tells you how to work with Document Types and Document Views.

- Chapter 12, *Importing Legacy Data*, tells you how to convert data from other applications such as Tivoli ServiceDesk or Knowlix to Get-Answers format.
- Chapter 13, *Using Best Practices*, describes the recommended ways to set up and use Get-Answers.

Contacting customer support

For further information and assistance with this release, contact Peregrine Systems' Customer Support.

Peregrine CenterPoint Web site

Current details of local support offices are available through the following main contacts or through the Peregrine CenterPoint Web site at:

<http://support.peregrine.com>

You need your current login user name and password to access this Web page.

To contact Peregrine customer support

- 1 Log in to the Web site with your login user name and password.
- 2 Click Go beside the CenterPoint support area.
- 3 From Contents on the left, select Whom Do I Call? to display the Peregrine Worldwide Contact Information.

Need further assistance?

For further information and assistance with this release, you can download documentation or schedule training.

Documentation Web site

For a complete listing of current Get-Answers documentation, see the Documentation pages on the Peregrine Customer Support Web site at:

<http://support.peregrine.com>

Access to this Web page requires a current login name and password.

Important: Release Notes for this product are continually updated after the release of the product. Visit the Peregrine Customer Support Web site to ensure that you have the most current version of the Release Notes.

To view the document listing

- 1 Log in to the Web site with your login user name and password.
- 2 Select **Get-Answers** from **My Products** at the top of the page.
- 3 From **Contents** on the left, select either **Documentation** or **Release Notes**, as required.
- 4 Follow the path for the Get-Answers product and version that you need.

You can download documentation PDF files and view them using Acrobat Reader, which is available on the Customer Support Web site and through Adobe at <http://www.adobe.com>.

Education Services Web Site

For a complete listing of Peregrine's training services, refer to the following web site:

<http://www.peregrine.com/education>

You can also call Peregrine training directly at +1 858.794.5009.

1 Architecture Overview

CHAPTER

Peregrine Open Application Architecture (OAA) platform is a software platform that enables the hosting of a variety of Web applications over a corporate intranet. The platform is Java based, encompassing the latest in Java technology including Java servlets, JAAS login authentication, and JSP pages that enable Web pages to display data dynamically.

Peregrine OAA Platform is the underlying architecture for many Peregrine products, including the Get-It suite of Employee Self-Service products which offers:

Get-It Product	Description
Get-Answers	Web-based, knowledge management application that enables you to capture and search on knowledge. Using Get-Answers, you can improve the quality and accuracy of the knowledge used by people in your company to get their jobs done and avoid calls to the help desk.

Get-It Product	Description
Get-Resources™	Web-based solution that integrates with AssetCenter Procurement, AssetCenter 4.x Portfolio, or ServiceCenter Request Management to enable employees to create requests for resources and to streamline the approval workflow of those requests throughout the organization.
Get-Services™	Web-based extension of ServiceCenter that enables users to report problems in the work environment by opening problem tickets in Get-Services and then storing them in the ServiceCenter back-end system, allowing users to view tickets from Get-Services and ServiceCenter. Modules include Administration, Service Desk, and Change Management (with ServiceCenter 5.0 and 5.1).

Peregrine OAA Platform provides a Web portal, Peregrine Portal, from which users can access their Web applications. The Peregrine Portal also provides access to the Admin module, from which all aspects of the Peregrine OAA Platform are monitored and maintained.

The base of Peregrine OAA Platform includes:

- Archway—a Java servlet that processes HTTP requests from a browser, sends the requests through an adapter to a back-end system, and returns XML data to be displayed in the browser.
- Core files—the Peregrine OAA Platform contains jsp and XML. The core consist mainly of low level Java utility classes used by the Portal Web applications built on the base OAA framework.
- Peregrine Portal—includes a login page and provides access to your Peregrine Web applications and to the Admin module for configuration of your application.
- Skins and style sheets—provide a choice for the appearance of the Web pages.

The Peregrine OAA Platform includes a number of optional components that are configured for use with Web applications as they are needed. These include:

- Adapters—enables connection to the back-end system database. The adapter required by your Web application is deployed during the installation.
- OAA Persistence (Get-Answers only)—provides a general purpose database that is used by certain Peregrine Web applications. OAA Persistence provides data persistence to a database.

- OAA Workflow (Get-Answers only)—enables workflow capabilities used by some Peregrine OAA Platform Web applications.
- Notification Services (Get-Answers only)—a centralized service for sending and receiving notifications through multiple communication devices and for tracking the status of these notifications.

Separate documentation for Notification Services is provided with the Web applications that use this feature.

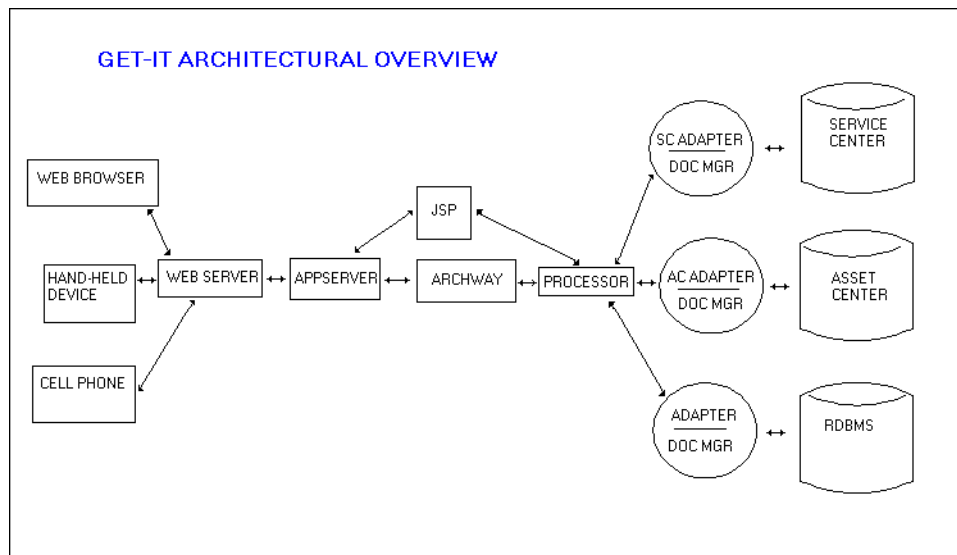
Peregrine OAA Platform architecture

Peregrine OAA Platform applications and interfaces use Web-based building blocks that include:

HTTP	A simple and widely supported protocol for sending client requests to a server. Variations such as HTTPS provide security as well.
XML	Extensible Markup Language. A documentation meta-language that allows you to format data, which can then be displayed through a Web browser. Unlike HTML, you create your own XML tags and define them any way you want.
Commercial web servers	The services provided by the Archway architecture can be served from any commercial Web server, including IIS and Apache.
Application servers	Peregrine OAA Platform supplies Apache Tomcat for an application server with the installation. JRun, WebSphere, and WebLogic are also supported.
Common clients	Applications can be deployed via Web browsers (IE, Netscape), handheld devices (Palm Pilot), or mobile phones (through HDML).

The application server processes data (JSP pages, XML, and so forth) that it receives from the database or client that is specifically related to the Peregrine Systems Web applications. The Web server converts the data into a form (HTML) that can be displayed in a Web browser.

The following diagram illustrates the architecture:



The Archway component listens to HTTP requests from clients, routes the requests to an appropriate server, and returns data or documents. The requests supported by Archway can vary, but they fundamentally consist of queries, data updates, or system events.

For example, a client can contact Archway and ask to query a database for a list of problem tickets. Another client could contact Archway and supply it with a new purchase request to be entered into the database.

All requests and responses are formatted using XML. For example, a problem ticket expressed in XML could appear as follows:

```

<problem>
  <number>PM5670</number>
  <contact> Joe Smith </contact>
  <description> My printer is out of paper </description>
</problem>
  
```

Clients that interact with Archway can do anything they need with the XML that is returned as a response. Very frequently, the client initiating the request is a user interface such as a Web browser. Such a client could easily display the XML documents returned by Archway. However, to be of better use, the XML documents are often displayed within a formatted HTML page. This is accomplished by using Java Server Pages (JSP).

JSP provides a syntax for creating HTML pages that is pre-processed by the Web server before being sent to the browser. During this processing, XML data obtained from Archway is merged into the HTML page.

Archway's architecture includes special support for automatically generating the HTML and JSP pages that make up a Web application.

Archway internal architecture

Archway is implemented as a Java servlet. The Java servlet is an application executed by a Web server that processes HTTP requests from client Web browsers and sends the request, by way of an adapter, to a database. It then retrieves the requested information from the database and returns it to the client. Archway requires both a Java environment and a Web server.

Each request is interpreted to determine its destination. Archway is able to communicate with a variety of back-end systems, including the AssetCenter or ServiceCenter products from Peregrine.

Requests can be handled in one of three ways:

- A request can be sent directly to an adapter that talks to a back-end server. For instance, a query request for opened tickets could be forwarded to an adapter capable of communicating with ServiceCenter.
- A request can be sent to a script interpreter hosted by Archway. This enables you to define your own application-specific services. Within a script, calls can be made back to Archway to access the back-end system with database operations and events.
- Finally, a request can be sent to a component known as a Document Manager. This component provides automated services for combining logical documents.

Archway communicates with back-end systems with the help of specialized adapters that support a predefined set of interfaces for performing connections, database operations, events, and authentication. All adapters use DLLs to communicate with each application.

Messages can be routed to a script interpreter hosted by Archway. The interpreter supports ECMAScript, a European standard based on the Core JavaScript language used by Netscape (JavaScript) and Microsoft Internet Explorer (JScript).

Messages can be routed to the Document Manager component. This component reads special schema definitions that describe application documents for logical entities such as a purchase request, problem ticket, or product catalog. The script interpreter uses these schemas to automatically generate database operations that query, insert, or update such documents.

Archway requests

Archway supports a variety of requests, all of which are based on two basic technologies: HTTP and XML. The HTTP protocol defines a simple way for clients to request data from a server. The requests are stateless and a client/server connection is maintained only during the duration of the request. All this brings several advantages to Archway, including the ability to support a large number of requests with the help of any of today's commercial Web servers.

Another important advantage is that any system capable of making HTTP requests can contact Archway. This includes Web browsers, of course. But in addition, all modern programming environments support HTTP. This makes it very simple to write new adapters that communicate with Peregrine servers without the need of specialized APIs.

You can test the output generated by your server-side onload scripts and schemas by using URL queries to the Archway servlet.

Archway will invoke the server script or schema as an administrative user and return the output as an XML document. Your browser will need an XML renderer to display the output of the XML message.

Note: Your browser may prompt you to save the XML output of the URL query to an external file.

URL Script Queries

Archway URL script queries use the following format:

```
http://server name/oaaservlet/archway?script name.function name
```

- For *server name*, enter the name of the Java-enabled Web server. If you are testing the script from the computer running the Web server, you can use the variable `localhost` as the server name.

The `/oaaservlet` mapping assumes that you are using the default URL mapping that Get-Answers automatically defines for the Archway servlet. If you have defined another URL mapping, replace the servlet mapping with the appropriate mapping name.

- For *script name*, enter the name of the script you want to run.
- For *function name*, enter the name of the function used by the script.

Note: URL queries functionality can be removed by configuring the `WEB.xml` file. This is a recommended security setting.

URL Schema Queries

Archway URL schema queries use the following format:

```
http://server name/oa/servlet/archway?adapter name.Querydoc
&_document=schema name
```

- For *adapter name*, enter the name for the back-end database adapter the schema uses. The adapter listed here will use the ODBC connection that you have defined in the Admin module Settings page.
- For *schema name*, enter the name defined in the <document name="schema name"> element of the schema file.

The `/oa/servlet` mapping assumes that you are using the default URL mapping that Get-Answers automatically defines for the Archway servlet. If you have defined another URL mapping, replace the servlet mapping with the appropriate mapping name.

URL SQL Queries

Archway URL SQL queries use the following format:

```
http://server name/oa/servlet/archway?adapter name.query&_table=
table name&field name=value&_[optional]=value
```

- For *adapter name*, enter the name for the back-end database adapter the schema uses. The adapter listed here will use the ODBC connection that you have defined in the Admin module Settings page.
- For *table name*, enter the SQL name of the table you want to query from the back-end database.
- For *field name*, enter the SQL name of the field you want to query from the back-end database.
- For *value*, enter the value you want to the field or optional parameter to have.
- For *_[optional]*, enter any optional parameters to limit your query. Examples include:

- `_return`. Returns the values only of the fields you list.
- `_count`. Specifies how many records you want returned with the query.

The `/oa/servlet` mapping assumes that you are using the default URL mapping that Get-Answers automatically defines for the Archway servlet. If you have defined another URL mapping, replace the servlet mapping with the appropriate mapping name.

The following are sample URL SQL queries:

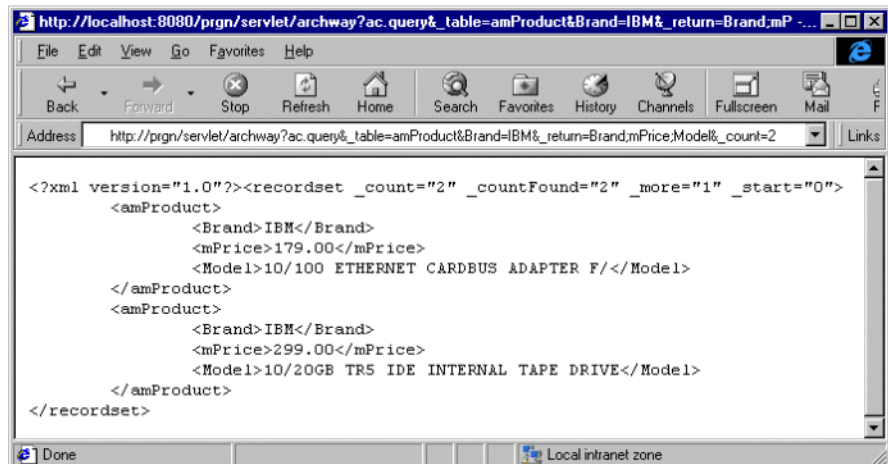
- `host name/oa/servlet/archway?sc.query&_table=probsummary&priority.code=1`

This sends a query request to ServiceCenter for all records in the probsummary table with a priority code of 1.

- `host name/oa/servlet/archway?ac.query&_table=amAsset&_return=Brand;mPrice;Model&_count=2`

This sends a query request to AssetCenter for the first two records in the amProduct table. Only the Brand, mPrice, and Model fields are returned for each record.

The screen below shows the XML results of a query for products from AssetCenter.



The Document Manager

Archway uses XML to exchange data and documents between clients and the supported back-end systems. Fundamentally, the XML data returned by Archway is obtained by executing queries against one or more systems. The queries can be executed by a direct URL request or indirectly within an ECMAScript function.

Simple queries are only capable of returning record sets of data. However, clients are more often interested in exchanging documents. A Document is a logical entity built up of several pieces of data that can come from various physical database sources.

The Document Manager uses schemas to determine which XML elements to use and what data should be contained in the elements. The data used by the Document Manager depends on the back-end system being used.

2 Setting-up Get-Answers

CHAPTER

Using Get-Answers, your company can store and access documents on any topic. Get-Answers creates a structure in which you assign users roles and capabilities so they can access this information. Before anyone can use Get-Answers, you must set up users and roles in the system. This chapter describes how to set up Get-Answers so users can work with Get-Answers.

Topics in this chapter include:

- *Users and roles* on page 28
- *Categories and document ownership teams* on page 45
- *Managing categories and document ownership teams* on page 47
- *Configuring Spider (Web crawler) files* on page 60
- *Using Crystal Reports with Get-Answers* on page 82

Users and roles

Users, roles, and capabilities work together to help users get their work done. Users are the people who use Get-Answers. Roles are the duties that users perform when working in Get-Answers. Capabilities are the rights or permissions that users have as they work in Get-Answers. This section describes users, roles, and capabilities in detail. The section *Managing categories and document ownership teams* on page 47 describes how to set up and maintain users, roles, and capabilities.

Users

There are three types of users: the Administrator (Admin), the Anonymous user, and the standard users.

Admin and Anonymous users

This section explains the Admin and Anonymous users, and how to add a password for these users the first time you launch Get-Answers. The Admin user and the Anonymous user perform all of the administration functions for Get-Answers.

Admin users

There are two types of Admin users. One is the OAA Admin user. This Admin user has the rights to configure Get-Answers.

The other is the Administration user that the Get-Answers adapters require to verify users against the database. This user is not a person but a permission that is passed to the database each time a user logs in so that the system can authenticate the user with the database. The Administration user can make changes for users in the database. For example, most users do not have permissions to change anything in the database through Get-Answers. If a user wants to change their password, the system must pass this information to the database. The Administration user interacts with and changes information in the database on behalf of a user.

In the first procedure on page 29, you add a password for the OAA Administration user. In the second procedure beginning on page 30, you add a password for the Administration user (Anonymous user) that interacts with the database.

Anonymous users

The scriptpollers that Get-Answers Workflow use require permissions. The Anonymous user provides those permissions.

In this second procedure on page 30, you can also add a name and password for the Anonymous user.

Important: For security reasons, you must change the password for each Administration user when you first launch Get-Answers.

Setting System Maintenance passwords

This section describes how to change the password for the System Maintenance administrator.

To change the System Maintenance user password:

- 1 Log in to Get-Answers using the **admin.jsp** page.
For example, go to `http://<servername>/oaa/admin.jsp`, where `<servername>` is your Get-Answers server name.
 - Enter **System** in the User Name field.
 - Leave the Password field blank.
- 2 Click **System Maintenance**.
The Control Panel page opens.
- 3 Click the **Settings** link on the left.
The Admin Settings page opens.
- 4 In **System Maintenance password:**, enter a password.
- 5 Scroll to the bottom of the page and click **Save**.
The Control Panel page opens.
- 6 Click **Reset Server** at the bottom of the page.
A confirmation message appears at the top of the page.
Note: Your changes do not take effect until you click **Reset Server** to reset the application server.

Setting Administration passwords

This section describes how to change the password for the Administration user and the administration user (anonymous users) that interacts with the database.

To add a password for the Admin and anonymous users:

- 1 Log in to Get-Answers using the login.jsp page. For example, go to `http://<servername>/oaa/login.jsp`, where `<servername>` is your Get-Answers server name.
 - In the Login Name field, enter **Admin**.
 - Leave the Login Password field blank.
- 2 Click **Login**.
- 3 Click the **People** tab.

The People Search page opens.
- 4 In the Login Name field of the People Search page, type **Admin**.
- 5 Click the **Search** button.

Note: If the People Search Results page opens first, find the Admin in the list. Go to step 6 without searching.
- 6 In the People Search Results page that opens, click the **Admin** link.

The Person Details page opens.
- 7 In the **Login Password** field, type a password for the Admin.
- 8 Click the **Submit Changes** button.

The People Search Results page opens and a confirmation message appears at the top of the page.
- 9 Click the **Administration** tab.
- 10 Click the **Settings** link on the left side of the page.

The Admin Settings page opens.
- 11 Click the **Get-Answers** tab.
- 12 Scroll down until you see the Administrator Password field.
- 13 In the **Administrator Password** field, enter the same password you used in step 7.
- 14 Scroll to the bottom of the page and click **Save**.

The Control Panel page opens.
- 15 Click the **Settings** link.

- 16 Click the **rome** tab.
- 17 In the **Anonymous Password** field, type the same password you used in step 7.
Note: On the rome tab, the Administrator password and the Anonymous password must match.
- 18 Scroll to the bottom of the page and click **Save**.
- 19 In the Control Panel page that opens, click **Reset Server**.
Note: Your changes do not take affect until you click **Reset Server** to reset the application server.

Important: If you change the Administrator user's password in the database via the People tab or when the Administrative user logs in, you must repeat step 9 through step 19. You should verify that the passwords on the Get-Answers tab (Administrator Password:) and the passwords on the rome tab (Admin password: and Anonymous Password:) are in sync.

Standard users

A standard user is any user who does not have OAA Administrator rights. These users log in at `http://<servername>/oaa/login.jsp` page, where `<servername>` is your Get-Answers server.

Once you have created an Administrator account and used this account to set up roles, you can start adding standard users to the system.

Roles

Roles groups users by capabilities, or rights. For example, the Editor role gives anyone assigned that role the permission to read, create, or update documents. The following roles are included with Get-Answers: Owner, Editor, Reviewer, and Reader. (See the sections, *Document ownership teams* on page 45, and *Managing categories and document ownership teams* on page 47 for more information.)

You can assign a user more than one role. Also, you can assign permissions to access the system to users, roles, or both.

Working with roles

As an administrator, you can create, modify, and delete groups of users by assigning them roles.

You see menu options that are used by other Peregrine Web applications in the People module, which is where Get-Answers users are managed. Only the menu options used by the Get-Answers web application are documented here.

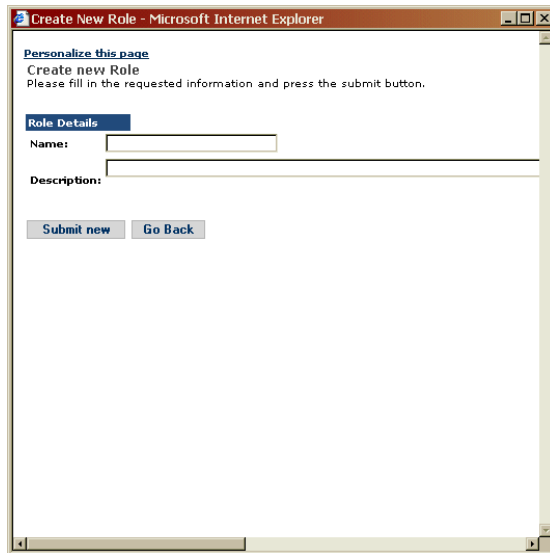
Adding roles

You add a role so that you can then associate users with the role and manage access to the documents in the system.

To add a role:

- 1 Click the **People** tab.
- 2 Click the **Functional Roles** link listed in Setup.
- 3 Click **New** to create a new role.

The Create New Role window opens.



The screenshot shows a web browser window titled "Create New Role - Microsoft Internet Explorer". The page content includes a "Personalize this page" link, the heading "Create new Role", and the instruction "Please fill in the requested information and press the submit button." Below this is a section titled "Role Details" with two input fields: "Name:" and "Description:". At the bottom of the form are two buttons: "Submit new" and "Go Back".

- 4 Enter a name for the role.
- 5 Enter a description for the role.
- 6 Click **Submit Changes** when you finish.

Modifying roles

Once you have created a role, you can modify the name or description of the role.

To modify a role:

- 1 Click the **People** tab.
- 2 Click the **Functional Roles** link listed in Setup.
- 3 Enter the role name and the description. Then click **Search**.

Note: You can click **View All** without entering the name for a list of all roles.

The Role Search Results window opens.

- 4 Select the role you want to modify.

The Role Details page opens.

- 5 In the Role Details page, make the desired modifications and click **Submit Changes**.

A confirmation message appears at the top of the Role Search Results page.

Deleting roles

You can delete roles from the system when they are no longer needed; however, when you delete a role you need to verify that any users accessing the documents in the system with the role you are deleting have other ways of accessing those documents or no longer need access to those documents.

To delete a role:

- 1 Click the **People** tab.
- 2 Click the **Functional Roles** link listed in Setup.
- 3 Enter the role name and the description. Then click **Search**.

Note: You can click **View All** without entering the name for a list of all roles.

The Role Search Results window opens.

- 4 Select the role you want to delete.

The Role Details page opens.

- 5 In the Role Details page, click **Delete** to remove the role.
- 6 Click **OK** in the delete verification message box.

A confirmation message appears at the top of the Role Search Results page.

Managing users and roles

An Administrator can add, modify, and delete users from Get-Answers. You can also assign users to roles, and you can assign as many users as you want to a role. You give the role and/or Document Ownership Team Permissions to a category.

Note: You may see menu options that are used by other Peregrine Web applications in the People module, which is where Get-Answers users are managed. Only the menu options used by the Get-Answers Web application are documented here.

Personalizing the Create New Person page

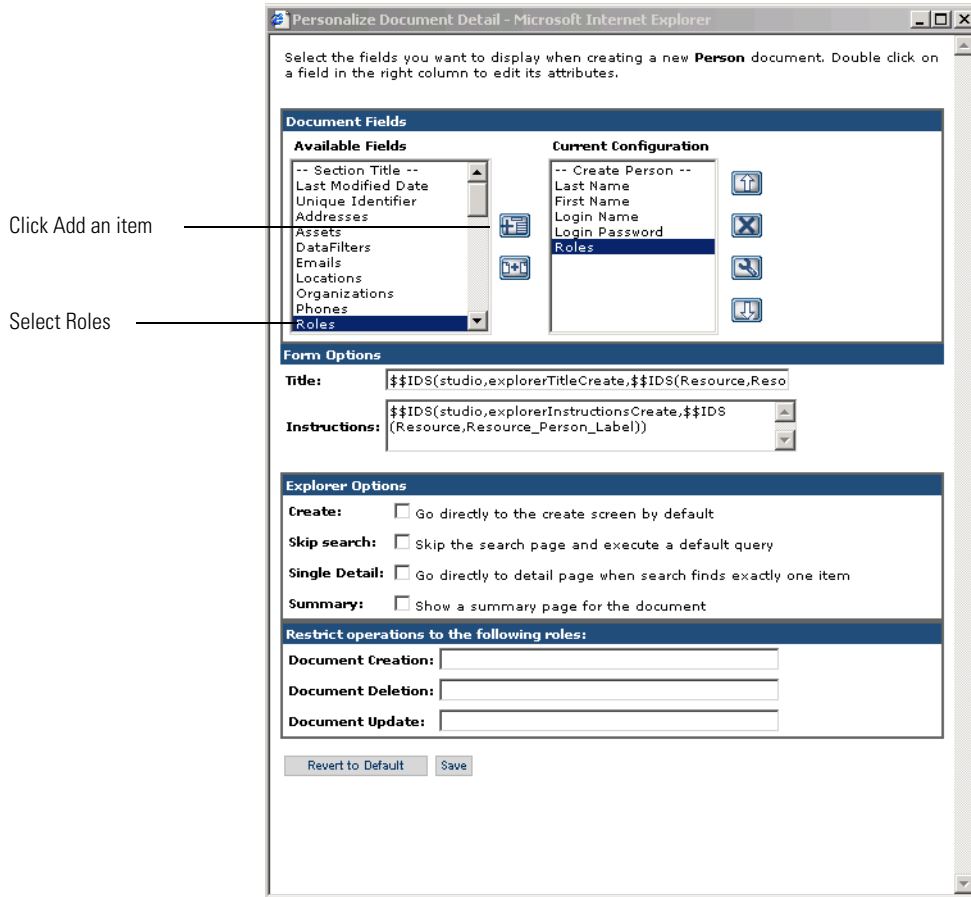
The default Create New Person page in the Peregrine Portal does not contain a hyperlink for adding roles for a user. Follow these instructions to set up the hyperlink now.

Note: For more information on using the Personalization interface, see *Chapter 5, Personalization*.

To add a hyperlink for adding roles to a user:

- 1 In the Peregrine Portal, click the **People** tab.
- 2 In the Person Search page, click **New**.
The Create New Person page opens.
- 3 In the Create New Person page, click the Personalize this page icon (wrench).
A Personalization window opens.

- In the Personalize Document Detail window, select **Roles** from the Available Fields list.



- Click the **Add an item** icon (plus sign).
Roles appears in the Current Configuration list.
- In current Configuration column, use the Move up or Move down icons (arrows) to select the position for **Roles** on the Create New Person page.
- Click **Save**.

The Create New Person page now contains the Roles: ([Add](#)) hyperlink.

The Roles (Add) hyperlink appears on the page.

The screenshot shows the 'Create New Person' page in the Peregrine Portal. The page has a header with the logo and navigation tabs for Home, People, Administration, Get-Answers, and Workflows. The 'People' tab is active. The main content area is titled 'Create New Person' and contains a form with the following fields: Last Name, First Name, Login Name, and Login Password. Below these fields is a 'Roles' section with an 'Add' hyperlink and a 'Remove' button. At the bottom of the form are 'Submit' and 'Go Back' buttons. A note at the top of the form says 'Please fill in the requested information and click the submit button.'

Adding users

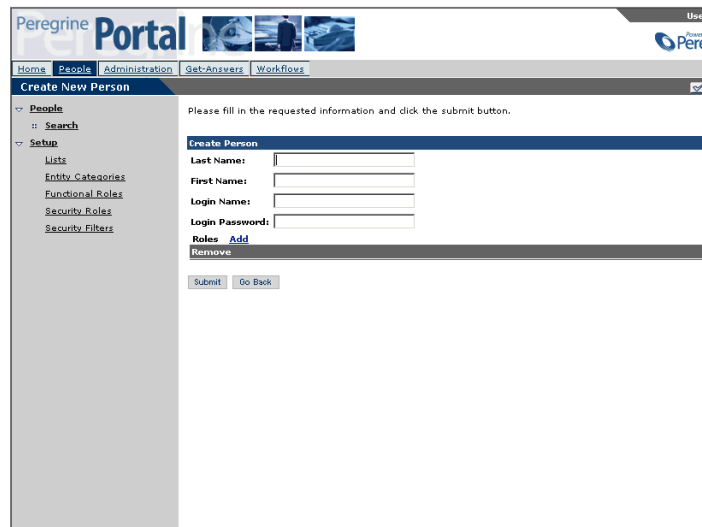
To add users to the system, you assign the user a login ID, password, and role in the system. A user's role determines the level of access the user has in the system.

To add a user:

- 1 In the Peregrine Portal, click the **People** tab.
- 2 In the Person Search form, click **New** to add a new user.

The Create New Person page opens.

Note: This illustration shows a Create New Person page with a personalized with a Roles: ([Add](#)) hyperlink as described in *Personalizing the Create New Person page* on page 34



- 3 Enter the Last Name and First Name for the user.
- 4 Enter the Login Name, and Login Password for the user.
- 5 To assign a user to a role, click Add next to Roles.

The Add New Roles page opens.



Note: Before you can do this, you must add the Roles: ([Add](#)) hyperlink as described in *Personalizing the Create New Person page* on page 34.

- 6 In the Add New page, click the search icon.
- 7 In the Lookup Role page, enter search criteria or leave Name and Description blank, and then click Search.

- 8 In the Lookup Role result table, click the selected role.



The role appears on the Add New Roles page.

- 9 Click **OK**.
- 10 Click **Submit Changes** to add the user.

The role(s) appears on the Create New Person page so you know the role (or group) that user belongs to.

Important: If you omit this step, the new user record is not saved.

Modifying users

Once a user has been added to the system, you can modify the user's profile by changing the roles assigned to the user.

To modify a user:

- 1 In the Peregrine Portal, click the **People** tab.
- 2 In the Person Search page, do one of the following:

- Enter the user's first name, last name, and login name. Then click Search.
 - Click View All for a for a list of all users.
- 3 In the Person Search Results page, click the name of the user you want to modify.

The Person Details page opens.

Please type changes and press the Submit button.

Person Details

Last Name:

First Name:

Login Name:

Login Password:

Roles [Add](#) [Lookup](#)

Remove	Name	Description
	Editor	

Login Capabilities:

Actions

[Set Security Capabilities](#)

- 4 Make the desired modifications. See [Adding users](#) on page 36 for more details.
- 5 To add or change the security capabilities assigned to this user, click Set Security Capabilities link.

The Set Security Capabilities page appears.

Please select from the list of available security elements.

Select	Capability	Description
<input type="checkbox"/>	Assets Management	Manage Assets
<input type="checkbox"/>	Assets Setup	Manage Assets Setup Details
<input type="checkbox"/>	People	Manage People
<input type="checkbox"/>	Organizations	Manage Organizations
<input type="checkbox"/>	Assign Role	Assign Roles to people
<input type="checkbox"/>	People Setup	Manage People Setup Details
<input type="checkbox"/>	Places	Manage Places
<input type="checkbox"/>	Places Setup	Manage Places Setup Details
<input type="checkbox"/>	System Maintenance user	Full access to system maintenance and administration activities.
<input type="checkbox"/>	Portal	Allow access to the Peregrine Portal
<input type="checkbox"/>	Personalization System Maintenance	Access to the system maintenance and administrative functions
<input type="checkbox"/>	Personalization default	Default capabilities for a Standard User
<input type="checkbox"/>	Get-Answers Administrator	View all Get-Answers Document Ownership Teams.
<input type="checkbox"/>	Get-Answers Reports	View all Get-Answers Reports.
<input type="checkbox"/>	Notification Services Administrator	Notification Services Administrator.
<input type="checkbox"/>	Notification Services GUI	Allow a user to view the Notification Services GUI.
<input type="checkbox"/>	Update Preferences	Allow a user to view and update their work schedule and device preferences in Notification Services.
<input type="checkbox"/>	Send Notifications	Allow a user to view the Send Notification activity in Notification Services.
<input type="checkbox"/>	View Notifications	Allow a user to view the Inbox and Outbox activities in Notification Services.
<input type="checkbox"/>	Workflow administrator	access to admin interface
<input type="checkbox"/>	Workflow Template designer	access to the designer interface
<input type="checkbox"/>	Workflow Process	add rights to edit a running process
<input type="checkbox"/>	Workflow Request	access to the request module
<input type="checkbox"/>	Workflow Standard User	basic access to the task list

Owners need this capability to create and edit forms.

- In the Set Security Capabilities page, click the check boxes next to a security capability to add or remove the capability, and then click **OK**.

Note: You need administrative capability to grant security capabilities to other users.

- Click **Submit Changes** when you finish.

Important: If you omit this step, the changes are not saved to the user record.

Deleting users

To delete a user:

- Click the **People** tab.
- You can search on the user's first name, last name, and login name. Then click **Search** to find the user you want to delete.

Note: You can click **View All** without entering the user's name for a list of all users.

- 3 Select the user you want to delete.
- 4 In the Person Details page, click **Delete** to remove the user from Get-Answers.

Capability keywords

This section describes how the capability words for menu items are used to control whether or not menu items display and examples of the roles capability keyword strings.

Menu item

For the menu item capability keyword for the Get-Answers tab, the out-of-the box are available as follows:

Get-Answers - `ga.document.read`; Admin, Owner, Editor, Reviewer, Reader, Submitter, Member

Search - `ga.document.read`; Admin, Owner, Editor, Reviewer, Reader, Submitter, Member

Browse Categories - `ga.document.read`; Admin, Owner, Editor, Reviewer, Reader, Submitter, Member

Contribute New Document - `ga.document.new`; Owner, Editor, Submitter

Manage Categories - `ga.domain.manage`; Owner (`ga.domain.create` to create New Categories; Owner)

Manage Document Ownership Teams - `ga.docteam.manage`; Admin, Owner (`ga.docteam.create` to create New Teams; Admin)

Manage Document Types - `ga.document.edit`; Owner, Editor

Import Documents - Roles.`ga._admin`; Admin user (Get-Answers Administrator check box on the Set Security Capabilities form)

Shared Content - `ga.document.own`; Owner, Editor

User Settings - `ga.document.read`; Admin, Owner, Editor, Reviewer, Reader, Submitter, Member

This screen image shows the menu items managed by the menu item capability keyword for the Get-Answers tab.



The following code is for the Reports menu items.

```
Reports - Roles.ga_rptview ; Admin user
Documents - Roles.ga_rptview ; Admin user
Document Feedback - Roles.ga_rptview ; Admin user
Usage History - Roles.ga_rptview ; Admin user
Search History - Roles.ga_rptview ; Admin user
Document Team Activity - Roles.ga_rptview ; Admin user
```

The following code is for the menu items on the Workflow tab:

```
Workflows - oaa.workflow.user; Admin, Owner, Editor, Reviewer, Reader
My Messages - oaa.workflow.user; Admin, Owner, Editor, Reviewer, Reader
My Requests - oaa.workflow.request; none
Templates Design - oaa.workflow.designer; Admin
Administration - oaa.workflow.admin; Admin
```

User and role capability keyword strings

Admin user capability keyword strings appended by Get-Answers to the *out-of-the-box* capability keyword strings:

```
Roles.ga_rptview;Roles.ga_admin;oaa.ns.admin;oaa.ns.gui;oaa.ns.preferences;
oaa.ns.send;oaa.ns.view;oaa.workflow.user;
oaa.workflow.designer;oaa.workflow.admin;oaa.workflow.processeditor
```

Owner role capability keyword strings:

```
ga.user.process;ga.document.read;ga.document.new;  
ga.document.edit;ga.document.own;ga.docteam.manage;ga.domain.manage;  
ga.domain.create;ga.domain.delete;oaa.workflow.user
```

Editor role capability keyword strings:

```
ga.user.process;ga.document.read;ga.document.new;ga.document.edit;  
oaa.workflow.user
```

Reviewer role capability keyword strings:

```
ga.user.process;ga.document.read;oaa.workflow.user
```

Reader role capability keyword strings:

```
ga.user.process;ga.document.read;oaa.workflow.user
```

Submitter role capability keyword strings:

```
ga.document.read;ga.document.new
```

Member role capability keyword strings:

```
ga.document.read
```

In the Person details form under the People tab, the Set Security Capabilities shows these two Get-Answers check boxes, which correspond to these capability keywords:

Get-Answers Administrator:

```
ga.docteam.admin;ga.docteam.create;ga.docteam.manage;ga.docteam.own;
ga.docteam.delete;ga.document.read;ga.documents.submit_batch
```

Get-Answers Reports:

```
Roles.ga_rptview
```

Buttons

Capability keywords also determine what buttons appear on a page. For example, `ga.document.own` is the permission necessary to see the Modify, Transfer, and Retire buttons in the Manage Document Screen window.

Direct Link to This Document: http://sames/aaa/login.jsp?bookmark=e_answers_kmSearchAlternate_basicSearch.jsp%3FdirectUrl%3Dtrue%26Id%3D1326%26format%3Dauthored

Document Metadata

Document Title: A licensing error appears when authoring RTF documents
Summary: The "localhost" URL does not support licensing.
Editorial Status: Published
Creation Date: 2003-8-1
Expiration Date: 2004-8-1
Date Last Modified: 2003-08-06T18:00:25+00:00

Review Feedback	Date	User Name	Delete this Comment
did not resolve the problem	2003-8-6	user, super	Delete: <input type="checkbox"/> Delete
incomplete documentation	2003-8-6	user, super	Delete: <input type="checkbox"/> Delete

Add Feedback

Was this document useful to you?

Yes
 No

Please type any feedback for the document owners here (2,000 character maximum)

Save Feedback and Close Modify Transfer Retire Close

ga.document.own is the necessary permission to view these buttons.

Categories and document ownership teams

Document ownership teams, which are groups of individuals in Get-Answers, manage categories. This section provides the concepts behind these key functions in Get-Answers.

Document ownership teams

Document ownership teams manage documents. Only one document ownership team owns a given document. You can transfer ownership of a document from one ownership team to another, but a document can never belong to more than one document ownership team at a time.

You can associate document ownership teams with any number of categories, but there is a single document ownership team for each category. This document ownership team becomes the owner of any new documents submitted to the category.

When a new document is submitted to a category, the category's ownership team is assigned as the ownership team of the document. Users with the permission owner within the document ownership team can transfer ownership of the document to another document ownership team, if appropriate.

Seven capabilities are defined within document ownership teams. These capabilities are used to define four permissions for document ownership teams. You can associate users or roles with one or more of the four permissions in a document ownership team.

The capabilities for document ownership teams include:

- Read — Can read working copies of documents.
- Create — Can create new documents.
- Update — Can check documents out, edit them, and check them back in.
- Revert — Can revert a document back to its published version and delete the working copy.
- Retire — Can retire documents.
- Publish — Can publish documents into any of the categories associated with the document ownership team.
- Transfer — Can transfer ownership of a document to another owner.

The roles and their capabilities within a document ownership team include:

- Owner — Read, Create, Update, Revert, Retire, Publish, and Transfer capabilities
- Editor — Read, Create, and Update capabilities
- Reviewer — Read and Review capabilities
- Member — Read published documents
- Submitter — Create new documents
- Reader — Read capability and author capability for ServiceCenter tickets.

In addition, owners, editors, and reviewers have particular responsibilities in the Editorial and /or Triage workflows. Readers play no part in the workflows. For information on workflows, see the [Chapter 10, Get-Answers Workflows](#) on page page 229.

Categories

A category is a grouping of published documents in Get-Answers. You can create categories by company department or another grouping method. For example, you can create a category in Get-Answers that contains all documents related to Human Resources.

Documents are published into categories. Categories can contain any number of documents. A document can belong to any number of categories. However, a new document can only be submitted to one category initially. It is then managed by the category's associated ownership team. A category is owned by one ownership team. Within categories, you can control the document hierarchy by creating categories for your documents.

A document cannot exist without being assigned to a category. This feature ensures that document ownership teams manage every document. No document is lost in the system because document ownership teams are always responsible for documents.

Within categories, there are two permissions. A category Member has read access to any document published to the categories. A category Submitter has read access to any document published into the category and can submit new documents to the category for review and possible publication by the categories document ownership team.

Managing categories and document ownership teams

Using the Manage categories menu option, a document team owner can add, modify, and delete categories from Get-Answers. Documents are published by categories, so by managing document categories you are actually managing how documents are grouped when they are published.

Working with categories

Categories group published documents by subject, department, or any other parameter you choose. Once you set up a category, you can divide it into subcategories. The following procedures describe how to add, change and delete categories and how to do the same for subcategories.

Adding, changing, or deleting categories

Use the following procedures to work with categories in Get-Answers.

Important: When you name categories, remember that category names cannot contain forward or backward slashes.

To add a category:

- 1 Click the **Get-Answers** tab and then click **Manage Categories** in the menu options.

The Search for Categories page opens.

Please enter the search criteria and click Search.

Name:

- 2 Click **New**.

The Category Detail page opens.

Type the new subcategory name and select the parent category. Click Insert.

Please enter the new Category and click Save.

Category Information

Name:

Description:

Managing Document Team:

- 3 Enter a Name for the category.
- 4 Enter a description of the category in the **Description** field.
- 5 Select the managing document team for the category.
- 6 Click Save.

The Category Detail page re-opens with additional detail. The Name, Description, and Document Team fields are filled in.

Please type changes and press the Submit button.

Category Information

Name:

Description:

Document Team Name:

Category Hierarchy

Type the new subcategory name and select the parent category. Click Insert.

New SubCategory:

Actions

[Set Submitter Permissions](#)

[Set Member Permissions](#)

- 7 In the Category Hierarchy section, type a New Subcategory.
- 8 In the Actions section, update the category permissions for the category by clicking the hyperlinks for submitter and member permissions (Set Submitter Permissions, Set Member Permissions).

In the Permission Detail page for submitter and member you can assign roles (group of users) or individual users to that particular permission for either a Submitter or a Member.

To add submitter permissions:

- 1 Click
- 2 For Submitter Permissions, click **Add Role** to assign a role (group of users) to this permission.
- 3 In the Search for Roles page, enter the role name you want to add and click **Search**.
- 4 Click the role and it appears on the Permission Detail page. Do this for as many roles as you want to add.
- 5 Click **Add User** to assign an individual user to this permission.
- 6 In the Search for Users page, enter the name of the user you want to add and click **Search**.
- 7 Click the user name and it appears on the Permission Detail page. Do this for as many users as you want to add.
- 8 Return to the category Detail page.
- 9 To control document hierarchy, you can add categories to the category. To add a new category, enter a name in the Category field and click **Add Category**.
Result: The new category appears in the list of category Categories.
- 10 To delete a category, select the desired category from the list and click **Delete Category**.
- 11 Click **Save Changes** when you finish.

Modifying categories

To modify a category:

- 1 Click the **Get-Answers** tab. Then click **Manage Categories** in the menu options.
- 2 Enter the category name. Then click **Search** to find the category you want to modify.
Note: You can click **Search** without entering the category name for a list of all categories.
- 3 Select the category. In the Category Detail page, make the modifications and click **Save Changes**.

Note: For details on the category options, see *Adding, changing, or deleting categories* on page 47.

Deleting categories

You can only delete a category or a subcategory that has not published documents in it and no subcategories.

To delete a category:

- 1 Click the **Get-Answers** tab. Then click **Manage Categories** in the menu options.
- 2 Enter the category name. Then click **Search** to find the category you want to delete.

Note: You can click **Search** without entering the category name for a list of all categories.

- 3 Select the category to delete.
- 4 In the Category Detail page that opens, click **Delete category** to remove the category.

Adding, changing, or deleting subcategories

Subcategories group documents in a category by subtype. For example, the category Human Resources could have subcategories of Payroll, Performance Reviews, and Time-Off Requests. This section explains how to work with subcategories.

In the following procedure, work with an existing category. (See *Working with categories* on page 47 to add categories.)

To add, change, or delete a subcategory:

- 1 From the Get-Answers Home page, click **Get-Answers**, and then click the **Manage Categories** link in the Get-Answers activity menu.
The Search for Categories page opens.
- 2 Enter a category, and click **Search**, or leave the field blank and click **Search** to see all categories.
- 3 Click the category you want in the list that opens.
The Category Detail page opens.

- 4 In the Category Detail page, find the Subcategory section, and click the category in the list on the right.

Go to the Subcategories section and select your category in the list.

Important: You must select the category in the list on the right before you can add a subcategory.

- 5 Do one of the following:
- To add a subcategory, type the new name in the Subcategory field and click **Add Subcategory**.
 - To delete a subcategory, click the subcategory in the list on the right and click **Delete Subcategory**.
- 6 Click **Save Changes**.

The message “Changes have been successfully saved” appears at the top of the page.

Adding submitter permissions for a category

Once you create a category or subcategory, you need to set submitter permissions for the category so users can use the category to manage documents. You can add submitter permissions by adding roles and adding users. A role gives a groups of users submitter permissions to the new category, or you can add a user to give an individual user submitter permissions.

Important: Users who have access to a category have access to all of its subcategories. You cannot assign users to specific subcategories.

To add submitter permissions to a category:

- 1 From the Get-Answers Home page, click **Get-Answers**, and then click the **Manage Categories** link on the left side of the page.

The Search for Categories page opens.

Please enter the search criteria and click Search.

Name:

- 2 Enter a category, and click **Search**, or leave the field blank and click Search to see all categories.

- 3 Click the category you want in the list that opens.

The Category Detail page opens.

Category Information

Name:

Description:

Document Team Name:

Category Hierarchy

Type the new subcategory name and select the parent category. Click Insert.

New SubCategory:

Actions

[Set Submitter Permissions](#)

[Set Member Permissions](#)

- 4 For the category information you select, click **Set Submitter Permissions**.

The Permission Detail page opens.

Click **Add User** or **Add Role** to assign Submitter permissions.

Submitter Permissions:

Name: Get-Answers

Submitter Permissions by Role

Remove	Roles
Add Role	

Submitter Permissions by User

Remove	Users
Remove	user, super
Remove	Owner, Otto
Remove	Editor, Ed
Remove	Reviewer, Rob

[Add User](#)

[Save](#)

- 5 To give submitter permissions to a role, click **Add Role**.
The Search for Roles page opens.
- 6 Enter the name of the role you are searching for and click **Search**, or click **Search** to list all the roles defined in the system.
The Role List page opens.
- 7 In the list, click the role you are adding to submitter permissions.
The Permission Detail page opens with the role you selected added.
- 8 Click **Save**.
You can continue to add roles for submitter permissions or individual users (next step) or
- 9 Click **Add User**.
- 10 In the Search for users page that opens, enter the user's first name, last name, or user login, and click **Search**.
- 11 In the List of Users page that opens, click the user's name in the list.
The Permission Detail page that opens, the user you've added appears on the list, and the message, "A user has been added to this permission" appears at the bottom of the page.
- 12 Click **Save** to return to the Category Detail page.
- 13 Click **Submit Changes**.

Adding member permissions for a category

Once you create a category or subcategory, you need to set member permissions for the category. When you set member permissions for a category you are giving read access to users or groups of users (roles) for all the documents in that category. You can add member permissions by adding roles and adding users. A role gives a groups of users member permissions to the new category, or you can add a user to give an individual user member permissions.

Important: Users who have access to a category have access to all of its subcategories. You cannot assign users to specific subcategories.

To add member permissions to a category:

- 1 From the Get-Answers Home page, click **Get-Answers**, and then click the **Manage Categories** link on the left side of the page.
The Search for Categories page opens.
- 2 Enter a category, and click **Search**, or leave the field blank and click Search to see all categories.
- 3 Click the category you want in the list that opens.
The Category Detail page opens.
- 4 For the category information you select, click **Set Member Permissions**.
The Member Detail page opens.
- 5 To give member permissions to a role, click **Add Role**.
The Search for Roles page opens.
- 6 Enter the name of the role you are searching for and click **Search**, or click **Search** to list all the roles defined in the system.
The Role List page opens.
- 7 In the list, click the role you are adding to member permissions.
The Member Detail page opens with the role you selected added.
- 8 Click **Save**.
You can continue to add roles for member permissions or individual users (next step) or click **Save** to return to the Category Detail page and click **Submit Changes**.
- 9 Click **Add User**.

- 10 In the Search for users page that opens, enter the user's first name, last name, or user login, and click **Search**.
- 11 In the List of Users page that opens, click the user's name in the list.
The Permission Detail page that opens, the user you've added appears on the list, and the message, "A user has been added to this permission" appears at the bottom of the page.
- 12 Click **Save** to return to the Category Detail page.
- 13 Click **Submit Changes**.

Working with document ownership teams

You can use the Manage Document Ownership Team link add, modify, and delete ownership teams from Get-Answers.

Note: You must have rights to create a new document ownership team. These rights should be part of the Admin role or in some cases you may need to make them part of the role that is responsible for managing the document ownership teams.

Use the following procedure to assign the rights to create or modify a document ownership team.

To grant get-answers capabilities to a user:

- 1 In Get-Answers, click the **People** tab.
- 2 Use the Search page that opens to find the person you want to give capabilities.
- 3 In the Person Details page that opens, click **Set Security Capabilities**.
- 4 Click the check box next to Get-Answers Administrator to place a check mark there.
- 5 Click **OK**.
- 6 In the Person Details page that reopens, click **Submit Changes**.

Adding document ownership teams

Each new document ownership team must have an owner. You create this owner by giving one of the users the *owner* permission for the team. The selected owner can then manage all other aspects of the team (give other users permissions, manage documents, etc.).

Note: After you create the new document ownership team, log off as Administrator and log in as the team owner and go to ‘Manage categories’ to create one or more categories and, if desired, categories of documents under the category.

To add a document ownership team:

- 1 From the **Get-Answers** tab, click **Manage Document Ownership Teams** link. The Search for Document Teams window opens.
- 2 Click **New**
The Document Team Detail page opens.
- 3 In **Name**, type the name of the new document ownership team.
- 4 Click **Save**.
The Permission Detail page opens.

Click **Add User** or **Add Role** to assign Owner permissions. An owner permission is required.

Owner Permissions:	
Name:	Technical Publications
Owner Permissions by Role	
Remove	Roles
<input type="button" value="Add Role"/>	
Owner Permissions by User	
Remove	Users
<input type="button" value="Add User"/>	
<input type="button" value="Save"/>	

- 5 Click **Add Role** to assign a role (group of users) to this permission.
- 6 In the Search for Roles page, enter the role name you want to add and click **Search**.
- 7 Click the role.
The role you select is listed on the Permission Detail page. Do this for as many roles as you want to add.
- 8 Click **Add User** to assign an individual user to this team.
The Search for Users window opens.
- 9 In the Search for Users window, enter the name of the user you want to add and click **Search**.

10 Click the user name.

The user name you selected appears on the Permission Detail page. Do this for as many users as you want to add.

11 In the Permission Detail page, click **Save**.

The Document Team Detail page opens.

12 Click **Submit Changes****13** Click **Save Changes** when you finish.


Important: Whenever you create a new document ownership team, you must set owner permissions for the new document team.

To set permissions for a document ownership team:

- 1 In the Actions section of the Document Team Detail page, click **Set Owner Permissions**.

Click on any of the Permission Actions to modify permissions.

Document Team Detail:

Name: 

Owned Categories

Name	Description
Technical Articles	

Actions

- [Set Owner Permissions](#)
- [Set Editor Permissions](#)
- [Set Reviewer Permissions](#)
- [Set Reader Permissions](#)

Click to set owner permissions.

The Permission Detail page opens.

Click Add User or Add Role to assign Owner permissions. An owner permission is required.

Owner Permissions:	
Name:	Technical Publications
Owner Permissions by Role	
Remove	Roles
Remove	Default
Remove	Manager

Click Add Role

Add Role

Owner Permissions by User	
Remove	Users

Click Add User

Add User

A role has been added to this permission.

Save

2 Click **Add Role**.

The Search for Roles page opens.

3 Click **Search** or type the name of the role.

The Roles List page opens.

4 Click the role from the list.

The Permission Detail page opens with the role you selected listed in the Owner Permissions by Role section.

5 Click **Save**.

The Document Team Detail page opens.

6 In the Actions section, click one of the following:

- Set Editor Permissions
- Set Review Permissions
- Set Reader Permissions

and repeat steps 2 to 6 until all permissions are set.

Note: You can use both add users and add roles to set up the permissions for the new document ownership team.

Modifying document ownership teams

To modify a document ownership team:

- 1 Click the **Get-Answers** tab. Then click **Manage Document Ownership Teams** in the menu options.
- 2 Enter the document team name. Then click **Search** to find the document team you want to modify.

Note: You can click **Search** without entering the document team name for a list of all ownership teams.

- 3 Select the desired document team. In the Document Team Detail page, make the desired modifications and click **Save Changes**.

Note: For details on document team options, see *Adding document ownership teams* on page 55.

Deleting document ownership teams

To delete a document ownership team:

- 1 Click the **Get-Answers** tab. Then click **Manage Document Ownership Teams** in the menu options.
- 2 Enter the document team name. Then click **Search** to find the document team you want to delete.

Note: You can click **Search** without entering the document team name for a list of all document teams.

- 3 Select the desired document team. In the Document Team Detail page, click **Delete Document Team** to remove the document team.

Note: If any documents or child categories exist for the document team you are deleting, the system does not allow you to delete the document team.

Configuring Spider (Web crawler) files

The following sections describe how to start and stop the Web crawler and automate and configure the Spider files. It also explains how to set up a firewall so that the Spider Web crawler is able to search the Web within the range of specified URLs and create an index, which then becomes available to users as part of the Get-Answers knowledge base and how to clear the KMspider indexes.

Note: Before you begin configuring the Spider files, you should first setup the Spider database. See *Setting Up the Web crawler*, in the *Get-Answers Installation Guide*.

Starting and stopping the Web crawler

You can start the Web crawler manually using the Get-Answers Search Engine System utilities.

To start or stop the Web crawler:

- 1 Manually start the spider processes.
 - a Unless the search engine server is already started as a service or running in a DOS window, start it by choosing **Start >Programs >Get-Answers Search Engine >Start Search Engine Search Server** and press **Enter** to exit the command prompt window.
 - b Choose **Start >Programs >Get-Answers Search Engine >System Utilities**.
 - c From the system utilities menu, select option 14, **GetAnswers Search Engine Internet Spider Utilities**.
 - d In the order listed on the menu, start the O2 server, then the URL server.
- Note:** Verify the O2 server is up and running in a separate DOS window before starting the other servers.
- e Start the Internet Spider support and processes (4 and 5), specifying the spider library, KMspider when prompted.

The search engine server dialog will display the URLs being crawled. Then the search engine will index these documents.

You can check the indexlog.dat file for an **INDEX COMPLETE** message.

- 2 Stop the spider processes.

- a From the system utilities menu (step 4b), select option 14, **GetAnswers Search Engine Internet Spider Utilities**.
- b Do the following:
 - Shutdown the Internet Spider and support processes <spider, tagent, tproc>.
 - Stop the url server.
 - Stop the O2 server.
- c Exit from **System Utilities** by entering a series of 1s.

Automating the Spider processes

The following section describes how to edit configuration files to set up the Spider to crawl and index automatically instead of running it manually through the system utilities menu.

To edit the `exec.cfg` file found in
`c:\<$USER_INSTALL_DIR$\peregrine\config:`

- 1 Before editing, make a backup copy of the `exec.cfg` file.
- 2 Using a text editor, open the `exec.cfg` file.
- 3 When setting up the processes:
 - Run the KMSpider processes in the following order at least one minute apart from each other: `urlserv`, `tagent_KMSpider`, `tproc_KMSpider`, and then `spider_KMSpider`.

Note: Starting on the left, the asterisks define the minute, hour, day of the month, month of the year, and day of the week.

In the following example, the `urlserv` is set to index every midnight and the subsequent processes are started one minute after each other

```
CRONTAB {
    EXECUTE "spider_KMSpider" "3 0 * * *";
    EXECUTE "tagent_KMSpider" "1 0 * * *";
    EXECUTE "tproc_KMSpider" "2 0 * * *";
    EXECUTE "urlserv" "0 0 * * *";
}
```

- 4 In the `CRON_PROG` statements for `spider_KMSpider`, `tagent_KMSpider`, and `tproc_KMSpider`, remove the `FLAGS INITIALLY_DEACTIVATED`; line.

```
CRON_PROG "spider_KMSpider" {
  COMMAND "${SPIDER_DIR}\bin\spider"
           "${SPIDER_DIR}\KMSpider/config/spider.cfg"      ;
  FLAGS INITIALLY_DEACTIVATED;
}

CRON_PROG "tagent_KMSpider" {
  COMMAND "${SPIDER_DIR}\bin\tagent"
           "${SPIDER_DIR}\KMSpider/config/spider.cfg"      ;
  FLAGS INITIALLY_DEACTIVATED;
}

CRON_PROG "tproc_KMSpider" {
  COMMAND "${SPIDER_DIR}\bin\tproc"
           "${SPIDER_DIR}\KMSpider/config/spider.cfg"      ;
  FLAGS INITIALLY_DEACTIVATED;
}

CRON_PROG "urlserv" {
  COMMAND "${SPIDER_DIR}\bin\urlserv"
           "-p 3127"      ;
}
```

- 5 Start the search engine and the O2 server of the Spider utilities. The Spider processes automatically run/index in the background at the times you specified.
- Unless the search engine server is already started as a service or running in a DOS window, start it by choosing **Start >Programs >Get-Answers Search Engine >Start Search Engine Search Server** and press **Enter** to exit the command prompt window.
 - Choose **Start >Programs >Get-Answers Search Engine >System Utilities**.
 - Select option 14, **GetAnswers Search Engine Internet Spider Utilities**.
 - Select option 2, **Start O2 server**.
 - Exit from **System Utilities** by entering a series of **1s**.

Spider configuration files

A Spider library has several configuration files.

- `spider.cfg` is the main Spider configuration file. All configuration for the Spider library is done in or linked through this file.

- `start.lst` is an optional file with a list of URLs to use as the starting points of the crawl.
- `permission.lst` specifies domains, hosts, directories, and extensions that Spider is allowed to process.
- `proxy.cfg` is only used if you have an HTTP proxy firewall. It contains proxy configuration options for crawling with an HTTP proxy. It specifies when to use direct connections (inside the firewall) and when to use the proxy (outside the firewall).
- `revisit.cfg` is an optional file that specifies how often previously visited URLs should be revisited.
- `forms.lst` is an optional file used to process forms and HTTP or FTP user authorizations.
- `cookies` is an optional file used to store state information between Spider and a host server.

spider.cfg

Note the following rules for the `spider.cfg` file:

- Any line beginning with a pound sign (#) is considered a comment line.
- Each command line lists the parameter name followed by a colon (:) and the value.
- If two values are given for the same parameter, the last value is used. No error is reported.
- Using unknown parameters produces no effect. If parameter names are misspelled or undefined, no error is reported.
- Parameter names listed with no parameter value (just white space) are considered empty and the default value is used, if one exists.

The parameters in the following chart must be set in `spider.cfg` directly. Edit the `spider.cfg`, in a text editor. Some of these parameters are already in `spider.cfg`, but they are deactivated by a pound sign (#) at the beginning of the line—which causes the default values to be used. To set a different value for one of these parameters, remove the pound sign from the line, and enter an appropriate value.

Parameter	Description
<code>afm_libpath</code>	Specifies the path to the AFM library files being used by Spider. The default is <code>SPIDERHOME/bin</code> .
<code>afm_loglevel</code>	Specifies the level of AFM processing detail you wish to store in the log file. Valid values are 0-4, where 4 is the highest level of information. The default is 0 (no logging).
<code>afm_lst</code>	Specifies the path to the <code>afm.lst</code> file being used by Spider. The default is <code>SPIDERHOME/spider-lib/config/afm.lst</code> .
<code>afm_rul</code>	Specifies the path to the <code>afm.rul</code> file being used by Spider. The default is <code>SPIDERHOME/afm.rul</code> .
<code>conn_timeout</code>	Specifies the number of idle seconds before Spider disconnects the socket connection to the HTTP/FTP server. The default is 20 seconds.
<code>follow_redirect</code>	Enables or disables URL redirect control: 1=automatically follow redirects encountered; 0=do not follow redirects. If you choose 1, the HTTP/HTTPS AFM automatically follows moved links until it encounters a URL that is not moved, or the maximum number of redirects (16) is reached. If you choose 0, the AFM marks the URL as “moved” and generates an HTML file with the redirected link as the output file. The default is 0.

Parameter	Description
<code>index_waiting_time</code>	<p>When the <code>storage_path</code> parameter is not specified, this parameter determines how long <code>tproc</code> should wait for the document handler to finish indexing the document when it is not stored locally. If the length of the document is larger than 1 MB, <code>tproc</code> will wait for the number of seconds calculated by the following formula (where <code>doc_length</code> is in KB):</p> $\text{index_waiting_time} * \text{floor}(\text{doc_length (KB)} / 256)$ <p>For example, if the <code>index_waiting_time</code> is 2 and the size of the document is 2 MB, then the waiting time is $2 * \text{floor}(2 * 1024 / 256) = 16$ seconds. The default is 2.</p>
<code>local_cookies</code>	Specifies how to manage cookies: 1=manage cookies locally (per module basis); 0=use cookies passed in as parameters. The default is 0.
<code>min_cache</code>	Specifies the minimum database cache size in megabytes. The default is 64.
<code>nfile_hashdbm</code>	Specifies the number of underlying database files for the VISDIS filter database. The default is 5.
<code>nsync_read_initurls</code>	Spider parses this number of starting URLs in the main thread and then starts the <code>tfetcher</code> (starts crawling). Spider then launches the thread to parse the rest of the URLs in the initial URL file. This thread will sleep for <code>waittime_nsync_read</code> seconds after it's done processing every <code>nsync_read_initurls</code> URLs. The default is 100.
<code>process_ftp_dirlist</code>	Enables or disables the FTP AFM: 1=convert the directory list transferred from the FTP site into an HTML file with the subdirectories as HTML links, which Spider can crawl; 0=disable FTP crawling. The default is 1.
<code>rware_name_server</code>	Specifies the host name and port number of a remote RetrievalWare (search engine) name server for Spider to connect to. (Example: <code>rware_name_server: rwhost:6000</code>)
<code>use_host_distance</code>	Enables or disables the host distance filter (<code>host_distance</code>). Use 1 or on, 0 for off. The default is 1.
<code>use_url_distance</code>	Enables or disables the distance filter (<code>url_distance</code>). Use 1 or on, 0 for off. The default is 1.

Parameter	Description
<code>verbose</code>	Specifies a level for the types of messages that appear in the log files for <code>tagent</code> and <code>tproc</code> . A message appears in the log file only if its assigned verbose level is less than or equal to this verbose level setting. The default is 0.
<code>waittime_nonsync_read</code>	See <code>nonsync_read_initurls</code> above. The default is 20 seconds.

start.lst

You can edit this file in a text editor.

If the crawl should begin at several URLs, parameter `initial_url` in the `spider.cfg` is set to the `start.lst` file. An example `start.lst` file follows:

```
#list of urls for initial_url:
http://www.convera.com/
ftp://ftp.example.com/
https://https.example.com/
```

url_distance

The `url_distance` parameter in the `spider.cfg` is the default maximum distance of all of the listed URLs. However, if a different maximum distance needs to be set for one or more of the URLs listed in the `start.lst` file, the `url_distance` parameter is listed immediately below the URL to which it applies. For example, if the `url_distance` parameter is set to 3 in the `spider.cfg`, but you want to restrict the crawl on `http://www.example.com/headlines/sports` to 2, the `start.lst` file would look like this:

```
#list of urls; all will use the default url_distance in the
spider.cfg
# except those URLs with a url_distance parameter below them.
#
http://www.convera.com
http://www.example.com/headlines/sports
url_distance: 2
http://example.com/recreation/
```

host_distance

You can also use the `host_distance` parameter along with the `url_distance` parameter in this file.

Host distance is very similar to URL distance. The only difference is that while URL distance starts counting down right from the starting URLs, host distance starts counting when Spider goes off of the starting host (the host where the starting URL resides). Spider will not crawl any further along the current sequence of URLs whenever either the `host_distance` or `url_distance` runs out.

For example, consider the following starting URL:

```
http://www.convera.com/  
url_distance: 50000  
host_distance: 0
```

In this case, the starting host is `www.convera.com`. With `host_distance` set to 0, Spider will not visit (nor will it follow any forward links of) any URL that does not start with <http://www.convera.com/>. If the `host_distance` is set to 1, Spider will crawl practically everything on `www.convera.com` and then all documents 1 link away from any pages on `www.convera.com`.

If the `host_distance` is set to 2, Spider will crawl practically everything on `www.convera.com` and then all documents 2 links away from any page on `www.convera.com`, and so on.

If, however, we had the following setting:

```
http://www.convera.com/  
url_distance: 2  
host_distance: 5
```

it is most likely that the `url_distance` will run out before Spider even gets to a document one link away from pages on `www.convera.com`. The `url_distance` is the limiting factor in this crawl.

permission.lst

You can edit this file using a text editor.

The purpose of the `permission.lst` file is to list the URLs that are allowed or disallowed on the crawl.

It is named in the parameter `permission_list_file` in the `spider.cfg` file.

Regular expressions are used to specify the URLs to crawl and index.

The following rules control which files Spider crawls:

```
allow
disallow
strong_allow
```

To allow URLs that match a regular expression, precede the regular expression with **allow**:. To disallow URLs that match a regular expression, precede the regular expression with **disallow**:. If no lines begin with **allow**;, all URLs are allowed. If a URL is matched by both an allow and a disallow, the disallow takes precedence. In other words, you can allow everything and override the exceptions with **disallow**. **strong_allow** works in reverse (it overrides disallow). In this case, you can disallow everything and override the exceptions with **strong_allow** statements.

You can also specify whether or not certain files are indexed using these indexing rules:

```
index_allow
index_disallow
index_strong_allow
```

These rules work exactly like the crawl rules, except they are applied after a file is fetched. For example:

```
allow: http://www.convera.com
disallow: /partners/
strong_allow: /solutions\.html$
index_allow: \.html$
index_disallow: /company/
index_strong_allow: /management\.html$
```

This example specifies that Spider should crawl the www.convera.com site, except for the partners directory, and crawl any URL ending with `solutions.html`, even if it is in the partners directory. (Note that a URL ending with `solutions.html` will not be crawled if it is not referenced by an allowed URL outside the partners directory.) The parameters then specify to index (amongst the files crawled) all HTML documents unless they are from the company directory. It further specifies to index any URL ending with `management.html`, even if it is found in the company directory.

Each rule in the permission list file is a set of regular expressions. A URL u matches a regular expression r if r matches any substring of u . The set of URLs $M(R)$ that matches a rule R is the set of URLs that match any regular expression r in R .

The set $A(S)$ of URLs allowed in any set of URLs S is

$$A(S) = S \text{ intersection } (M(\text{strong_allow}) \text{ union } (M(\text{allow}) \text{ minus } M(\text{disallow})))$$

where **strong_allow** is the strong allow rule, **allow** is the allow rule and **disallow** is the disallow rule.

Suppose there is no URL and host distance limitation. Let S be the set of URLs in the `start.lst`. The set A of URLs that Spider crawls is determined by the following recursive rule:

- 1 $A(S)$ belongs to A
- 2 If u belongs to A and $\text{links}(u)$ is all the URLs referenced by u , then all URLs in $A(\text{links}(u))$ belong to A
- 3 No other URLs belong to A .

Following is an example of a `permission.lst` file.

```
# Copyright 1999-2002 Convera Technologies, Inc.
#-----
# * All comments start with #
# * All blank lines are not processed
# SYNTAX: strong-allow: <URL extended regex pattern>
# allow: <URL extended regex pattern>
# disallow: <URL extended regex pattern>
# RULES:
# (1) If no allow field is given, it is assumed that all URLs are
# allowed.
# (2) If no disallow field is given, no URLs are disallowed.
# (3) Disallows take precedence over allows but not over
# strong-allows.
# (4) Strong-allows will override disallows and guarantee the URL
# matching
# the regex will be crawled.
# Commonly used regular expression patterns:
# ^ beginning of line
# $ end of line
# \ escape -- make following character literal, no special meaning
# . any single character
# * zero or more of the PRECEDING character (or class)
# + one or more of the PRECEDING character (or class)
# ? zero or one of the PRECEDING character (or class)
# [] character class -- any one of the contained characters or range
# [^] character class -- any one character NOT in the class or range
# This example file allows the following URLs to be crawled:
# (1) http://www.yahoo.com/Entertainment/*
# (2) *.html, *.htm (case insensitive)
# (3) *.text, *.txt (case insensitive)
# (4) */ (URLs ending with a slash; i.e. directories)
# (5) */ (a sequence of characters without a '.'; i.e. files without
# extensions)
```

```

# Except (2) - (5) have the following restrictions:
# (1) */bin/*
# (2) */cgi-bin/*
# (3) ** (decorated URLs that pass variables to forms)
# (4) *netscape.com*
# (5) *www.yahoo.com*
strong_allow: www\.yahoo\.com/Entertainment/
allow: \.[Hh][Tt][Mm][Ll]?$
allow: \.[Tt][Ee]?[Xx][Tt]$
allow: \.[Dd][Oo][Cc]$
allow: \.[Pp][Dd][Ff]$
allow: /$
allow: /^[^.]+$
disallow: /bin/
disallow: /cgi-bin/
disallow: [?]
disallow: netscape.com
disallow: www\.yahoo\.com # The strong-allow above still
# allows Entertainment/ to be crawled.
# Technically, the above example only crawls the specified URLs.
# Indexing the pages is controlled by another set of keywords:
# index_allow, index_disallow, index_strong_allow
# These keywords follow the same syntax and rules as the basic
keywords,
# so leaving them out of the file would result in all crawled pages
being
# indexed (by Rule 1). Note that pages must be crawled before they
can be
# indexed.
# Often the indexing keywords are used to prevent indexing of pages
that
# are uninteresting for their content, but are important to the
continuation
# of the crawl.
index_disallow: /links\.html?$

```

Crawling SHTML files

Spider can retrieve and index SHTML files, if you add the following rule to the `permission.lst` file:

```
allow: \.[sS][hH][tT][mM][lL]?$
```

proxy.cfg

You can edit this file in a text editor.

The `proxy.cfg` file is an HTTP proxy firewall configuration file associated with the `proxy_connection_config` parameter in the `spider.cfg` file. You need to set up the file only if you have an HTTP proxy firewall (not if you have a SOCKS firewall). It is used to determine whether a URL should be fetched by

the HTTP proxy server or by direct connection. If `proxy_connection_config` specifies a file and that file is left empty, then all URLs will be retrieved through the HTTP proxy server. See *Firewall setup* on page 79 for more information.

To directly fetch a URL that matches a regular expression, precede the regular expression with **direct:** in the `proxy.cfg` file. To use the HTTP proxy server to fetch a URL that matches a regular expression, precede the regular expression with **proxy:.** If a URL is matched by both a direct and a proxy statement, the proxy statement has priority.

For example, below is a `proxy.cfg` file where all traffic going to `convera.com` will be via direct connection while traffic going to `example.com` will be through the HTTP proxy server.

```
# Convera Internet Spider Proxy Configuration
direct: convera.com
proxy: example.com
```

revisit.cfg

You can edit this file in a text editor.

The purpose of the `revisit.cfg` file is to set a schedule to revisit the URLs that have already been visited. The file is named in the `revisit_control_file` parameter of the `spider.cfg` file.

Below is an example of `revisit.cfg`:

```
#-----
# Transfer Frequency Control File
#-----
# The following parameters are in days
# Number of days to wait before attempting to crawl a
# URL that had not changed last time.
no_change_revisit: 0
# Number of days to wait before attempting to crawl a
# URL that had changed last time.
change_revisit: 0
# Number of days to wait before attempting to crawl a
# URL that was not found last time.
extinct_revisit: 0
# Number of days to wait before attempting to crawl a
# URL that had been moved last time.
moved_revisit: 0
# Number of days to wait before attempting to crawl a
# URL that timed out during trnasfer last time.
timed_out_revisit: 0
# Number of days to wait before attempting to crawl a
```

```

# URL that encountered a transfer error the last time.
transfer_error_revisit: 0
# Number of days to wait before attempting to crawl a
# URL for which access was denied the last time.
access_denied_revisit: 0
#-----
----
# Special Revisit configuration
# The precedence is in reverse order of entry. So if there is a
# conflict, the last setting takes precedence
#-----
----
#retrieve_frequency: 5: http://www\example\.com/
#retrieve_once: http://www.example.com/icons/2s_abt.jpg
#retrieve_always: http://www\example\.com/prods.html$
#retrieve_normal: http://www\example\.com/client.html$

```

There are two types of revisit timers: general (for all URLs), and specific. You can set how often all URLs should be revisited and reprocessed by setting the general timing parameters. To control how often a specific set of URLs are revisited, set the specific timing parameters. The parameters that can be set for these timers are listed in charts in the next two sections.

Timing parameters should be entered from general to specific. In the `revisit.cfg` file, general timers should be placed first, followed by the specific timers. The precedence is in reverse order of entry in the file. If there is a conflict, the last setting takes precedence.

General revisit timers

General revisit timers indicate the number of days (fractional days are allowed) to wait before revisiting URLs. Use these timers if your system contains one Spider library or if it contains multiple Spider libraries that do not visit the same sites. If you are crawling over multiple libraries that may be crawling the same sites, you may wish to use only the specific timer `retrieve_always`. (See the next section *Specific revisit timers* for more information.)

If the `revisit.cfg` file does not exist, the timers will be set to the default values given in the chart below. Use these parameter descriptions to modify the sample `revisit.cfg` file for your crawl:

General Revisit Timers for all URLs

Parameter name	Default (days)	Description
<code>change_revisit</code>	1	URLs that were new or had changed on the last visit.
<code>access_denied_revisit</code>	5	URLs that were denied due to invalid or no user ID or password.
<code>extinct_revisit</code>	30	URLs that were marked bad by HTTP return code (404, for example) on the last visit.
<code>moved_revisit</code>	0	URLs that were marked moved by HTTP return code (301, 302) on the last visit.
<code>timed_out_revisit</code>	5	URLs that timed-out during the last transfer.
<code>transfer_error_revisit</code>	5	URLs with transfer errors other than timing out (couldn't connect, couldn't find host, and so on) during the last transfer.

Specific revisit timers

Specific revisit timers affect a specific set of URLs through special regular expression directives similar to how the `permission.lst` works. The chart that follows contains a list of the directives and their meaning. Each directive should be followed by a colon (`:`) and a regular expression that matches the URLs for which this directive applies.

If you have multiple Spider libraries, in order to crawl and index URLs that have already been visited for another library, set `retrieve_always` to `"retrieve_always:.*"` and do not set the other specific timers. This change ensures that no documents will be skipped during the crawl, but it also may cause the crawl to take longer.

Use the parameter descriptions in the chart below to modify the sample `revisit.cfg` file for your crawl:

Specific Revisit Timers for Specified URLs

Parameter name	Default (days)	Description
<code>retrieve_once</code>	none	Retrieve the URLs that match the regular expression only once during the lifetime of the Spider database.
<code>retrieve_always</code>	none	Retrieve and re-index URLs that match the regular expression on every crawl.
<code>retrieve_frequency: #:</code>	none	Retrieve the URLs that match the regular expression at the specified interval where “#” is the minimum number of days between transfers of a URL. For example, <code>retrieve_frequency: 5.0:</code> <code>http://www.example.com/</code> means retrieve the “example site every 5 days.
<code>retrieve_normal</code>	none	Normally retrieve the URLs that match the regular expression; that is, use the rules from the general timers. If the general timers are all 0 (expired) then the URLs will be visited and indexed on every crawl. This parameter is intended to be used for exceptions to a more abstract regular expression.

For example, the following parameters mean that everything on the “example” site should be crawled every five days. GIFs and JPEGs are transferred only once, `today's_news.html` are transferred every crawl and all of the files in the `/Example/` directory are transferred using rules in the general timers.

```
retrieve_frequency: 5.0: http://www.example.com/
retrieve_once: \.[gG][iI][fF]$
retrieve_once: \.[jJ][pP][eE]?[gG]$
retrieve_always: ^http://www.example.com/today's_news.html$
retrieve_normal: ^http://www.example.com/Example/
```

If a URL is not crawled because its revisit time has not yet arrived, its forward links are still followed.

forms.lst

Spider can automatically fill out forms and can provide an ID and password to hosts that request authentication. Forms and authorization are configured through a file called `forms.lst`. You only need to include this file if you will be processing web forms. The file is named in the `form_file` parameter in `spider.cfg`. We recommend the form file listed in parameter `form_file` be located in the following directory: `ware/spider/ libname/config/forms.lst`.

Copy the sample `forms.lst` file from `rware/spider/sample/config/forms.lst` to your library directory `rware/spider/ libname/config/forms.lst` and use it as a starting place. Edit it to your specific needs. Remember to obtain IDs and passwords from sites whose forms you will be processing. You may list any number of sets of values for a form, and the Spider will crawl all of them.

CGI forms submission

To use the automatic forms submission feature, you must be familiar with the HTML `<form>` syntax. For more information, see “Mosaic for X version 2.0 Fill-Out Form Support” at the following site:

<http://www.ncsa.uiuc.edu/SDG/Software/Mosaic/Docs/fill-out-forms/overview.html>

When using the automatic forms submission feature, you must also set up the following:

- 1 In the `permission.lst` file, insert the following line, because all processed form URLs will end in

```
FORM:
allow: FORM$
```

- 2 In the `revisit.cfg` file, set both of these parameters to 0:

```
transfer_error_revisit: 0
timed_out_revisit: 0
```

The following is the syntax of the configuration parameters in `forms.lst` for automated forms submission:

```
form: regular expression for the URL for form 1
submit: submit button value to be used for form 1
field: field name 1= value1
field: field name 2= value2
form: regular expression for the URL for form 2
submit: submit button value to be used for form2
field: field name 1= value1
```

.
.
.
etc.

The **field:** value corresponds to the name field of each <input> syntax and the **submit:** value corresponds to the value field of <input type=submit value="...">.

Whenever a URL is transferred, it is compared against the regular expression in the **form:** field. If there is a match, then the HTML page is parsed and all of the <FORM>s are extracted. All fields are set to their default values unless specifically set in the field: parameters. The **submit:** field must exist since it is the mechanism by which Spider distinguishes between different forms on the same HTML page.

Currently there is no support for de-selecting default selections in multiple-select objects such as check-boxes and multi-select boxes.

For example, below is the section of a forms.lst file that automates filling out a form.

```
#-----
# This feature provides a way to crawl password protected sites
# through a simple CGI forms type of login and HTTP user
# authorization
# It will work only with forms pages that have 1 form on them.
# NOTE: You can also crawl most password protected sites through the
# use of the cookies feature.
#####
#-----
# forms based login into Example_Site
#-----
form: ^http://www\.example_site\.com/auth/login
submit: " Continue"
field: User="your_company"
field: Password="password1"
field: SAVE=PASSWORD
```

Setting authorization

The user authorization feature is the most common way of crawling password protected sites. Normally when you're using a browser, a window will pop up to ask your user name and password before accessing a certain page. For more information about authorization, see the following site:

<http://www.w3.org/Protocols/HTTP/1.0/spec.html#Authorization>.

User authorization is set in the `form.lst` file with the following format:

```
authorization: regular-expression user-ID: password
```

When a URL matches the regular expression given in the first argument, the user ID and password are given to the HTTP server. Notice the regular expression and ID: password must be separated by a space. The user ID and password are actually a united field used for the authorization. They must appear on the same line (not broken by blanks, carriage returns, or any other characters). Spider only supports the “basic” authorization method.

For example, below is the section of a `forms.lst` file that sets authorization.

```
#-----
# User authorization based login
#-----
authorization: www\.example2000\.com/~wsapi/investor/
my_name:my_passwd
```

You can also set up FTP user authorization information in the `forms.lst` file. For example:

```
authorization: www\.example2000\.com/~wsapi/investor/
my_name:my_passwd
```

- The FTP login information is determined as follows:
- If the URL contains user information, use it (as in, `ftp://user:passwd@ftp.example.com/`).
- Otherwise, use the user information in the authorization configuration file, if a match is found.
- If no login information is found in those two sources, the user is “anonymous” and the password is the “From” parameter in the main configuration file.

cookies

A cookie is a piece of limited, internal information transmitted between the host server software and the browser application. This is an optional file to initialize and save the cookies used by Spider. If the cookie file is not provided, Spider still sends and receives cookies, but the cookies will not be saved when the server is shut down. **tagent** reads the cookie file at startup time and saves cookies when it shuts down.

We do not provide a sample cookie file, but you should be able to copy the cookie file from your browser if you want to give Spider a initial cookies file. For example, if you don't want to store authorization information in `forms.lst`, you could authorize yourself through Netscape and use the Netscape cookie file to start the crawl. The file is named in the `cookie_file` parameter in `spider.cfg`.

Extended regular expressions reference

Regular expressions are used in the following configuration files:

`permission.lst`

`proxy.cfg`

`revisit.cfg`

`form.lst`

The following chart shows commonly used extended regular expressions. Solaris users can also refer to “`man -s 5 regex`” man pages.

Characters	Meaning	Example
<code>^</code>	Regular expression must match from the beginning of the string.	<code>^http :</code> matches all strings beginning with <code>http :</code>
<code>\$</code>	Regular expression must match at the end of the string.	<code>html\$</code> matches all strings ending in <code>html</code>
<code>\</code>	Negates all special meaning for the following character.	<code>\\$</code> matches the <code>\$</code> character
<code>.</code>	Matches any 1 character	<code>welcome.</code> matches <code>welcome1</code> , <code>welcomeb</code> , <code>welcome?</code> and any other string with <code>welcome</code> followed by any 1 character
<code>*</code>	Matches 0 or more of the preceding characters.	<code>welcome*</code> matches <code>welcom</code> , <code>welcome</code> , <code>welcomee</code> , <code>welcomeee</code> , etc.
<code>+</code>	Matches 1 or more of the preceding characters.	<code>welcome+</code> does not match <code>welcom</code> , but does match <code>welcome</code> , <code>welcomee</code> , <code>welcomeee</code> , etc.
<code>?</code>	Matches 0 or 1 of the preceding characters.	<code>html?</code> matches only <code>htm</code> and <code>html</code> .

Characters	Meaning	Example
[]	All characters within the []s are considered to be a character class. It will then match any single characters contained within the []. All characters lose their special meaning within the [^].	[a-zA0-9\n] matches all alphanumeric characters plus the carriage return.
[^]	All characters within the []s are considered to be a character class. It will then match any single character not contained within the [^]. All characters lose their special meaning within the [^].	[^a-zA-Z0-9\n] matches all characters except for alphanumeric characters and a carriage return.

Firewall setup

Spider supports two kinds of firewalls:

- SOCKS (UNIX only)
- HTTP proxies (both UNIX and NT)

Determining your firewall type

You can usually find out what kind of firewall you have from your network administrator. If the administrator is not available, check for the following:

- 1 If you have an `/etc/socks.conf` file then you most likely have a SOCKS firewall.
- 2 You can also look in your Netscape browser's network proxy configurations to determine the kind of firewall you have. If your HTTP Proxy field is set, then you should use the HTTP proxy parameters. If your SOCKS "Host:field" is set, then you should choose the SOCKS option.

SOCKS setup

You will need to set the `SOCKS_SERVER` environment variable to the IP address (not the hostname) of the machine that your SOCKS server is running on.

For example, if your `SOCKS_SERVER` is running on host `proxy.mycompany.com`, you can find out the IP address like this:

```
> telnet proxy.mycompany.com
Trying 123.45.67.8...
```

The IP address in this case is 123.45.67.8. You will then need to set the environment variable `SOCKS_SERVER`. The command you use depends on what shell you use:

Shell	Command
<code>csh</code> or <code>tcsh</code>	<code>> setenv SOCKS_SERVER 123.45.67.8</code>
<code>ksh</code> or <code>bash</code>	<code>> export SOCKS_SERVER=123.45.67.8</code>

HTTP proxy setup

The HTTP proxy support is toggled on and off through three parameters set in the `spider.cfg` file:

`proxy_host`, `proxy_port`, and `proxy_connection_config`.

If either the `proxy_host` or `proxy_port` parameters are not set, then this feature is disabled. All of these parameters are located in the `spider.cfg` configuration file. The `proxy_connection_config` specifies an additional configuration file, `proxy.cfg`, that defines when to use the proxy.

Clearing KMspider indexes

If necessary, you can clear the all the indexes/URLs in the Spider database.

To clear KMspider indexes:

- 1 Stop all Spider processes and the search engine.
- 2 Open a command prompt and type `dbmanage -dbclean`.
- 3 In the system utilities menu, delete and clear indexes for KMSpider.
- 4 In the system utilities menu, delete any log files as needed.

Integrating Get-Answers with AssetCenter

The information in this section is intended only for administrators who are configuring Get-Answers to work with Peregrine's AssetCenter, an asset management product.

Integrating Get-Answers in AssetCenter enables you to search the Get-Answers knowledge base. This integration is available in Get-Answers versions 4.0 and higher.

Note: The integration is functional only if the user has local administrative rights on the client computer.

To use the integration:

- 1 Copy and execute the file, `jcinst.exe`, on the Get-Answers server and then copy and execute this file on each client that will access Get-Answers.

This file is usually located in the following folder:

`c:\Program Files\Peregrine\Common\Tomcat4\webapps\oaa\integrations\`

- 2 Follow the installation instructions given by the program, `jcinste.exe`.
- 3 Start your Web browser with the following address:

```
http://<Get-Answers  
server>/oaa/login.jsp?_bookmark=e_answers_kmSearchAlternate_basicSearch.jsp?D  
DEType=SC
```

This completes integration of AssetCenter with Get-Answers.

Using Crystal Reports with Get-Answers

You can use Crystal Reports to provide summary reports and metrics relating to how the Get-Answers application is being used by your organization. The installation CD contains four reports meant for out-of-box use or customization by your Crystal Reports administrator. The four reports are:

- Document Usage Metrics - this report identifies the documents most often accessed and provides metrics relating to the usefulness of each document.
- Document Team Performance Metrics - this report shows number of documents published by document team and includes metrics for documents modified, submitted, and retired.
- User Performance Metrics - this reports shows how individual users accessed documents and includes metrics for queries, documents read, and user feedback.
- Document Users, Usage Metrics - this reports shows which documents users accessed most often, and how they rated the usefulness of these documents.

Each report is self-contained, has a prompt for usage and date range, has standardized formulas, and has an ERD. The reports can be exported and published in html.

In order to use these reports you need to:

- Have the Crystal Reports application.
- Copy the four files (.rpt) from the **sample reports** folder within the **documentation** folder on the installation CD to a server/directory where Crystal Reports can access them.
- Set up an ODBC connection between Crystal Reports and your Get-Answers Oracle database.

3 Using the Peregrine Portal

CHAPTER

The Peregrine Portal includes a Navigation menu, an Activity menu, and buttons that enable you to customize your Portal and to end your session.

Your installed Web applications determine the contents of the Navigation menu. However, if you log in as an administrator, all Navigation menus include an Administration tab that provides access to the Admin module.

The graphics in this chapter use the Classic stylesheet and are examples of a generic interface. Also, the Admin module displays only those features that Get-Answers uses. For more advanced changes to the portal, see the chapter on *Customizing the Peregrine Systems Portal*.

Topics in this chapter include:

- *Logging in to the Peregrine Portal* on page 84
- *Using the Activity menu* on page 85
- *Personalizing the Peregrine Portal* on page 86

Logging in to the Peregrine Portal


There are two login screens that provide access to the Peregrine Portal:

- A user login screen—`http://<server>/oaa/login.jsp`
- An administrator login screen—`http://<server>/oaa/admin.jsp`

Note: An alternative to this login method is the Integrated Windows Authentication. See the *Security* chapter of this guide.

This chapter discusses the features available with a user login. For more information about the administrator login, see the chapter on *Get-Answers Administration* in this guide.

The following is an example of the user login interface.

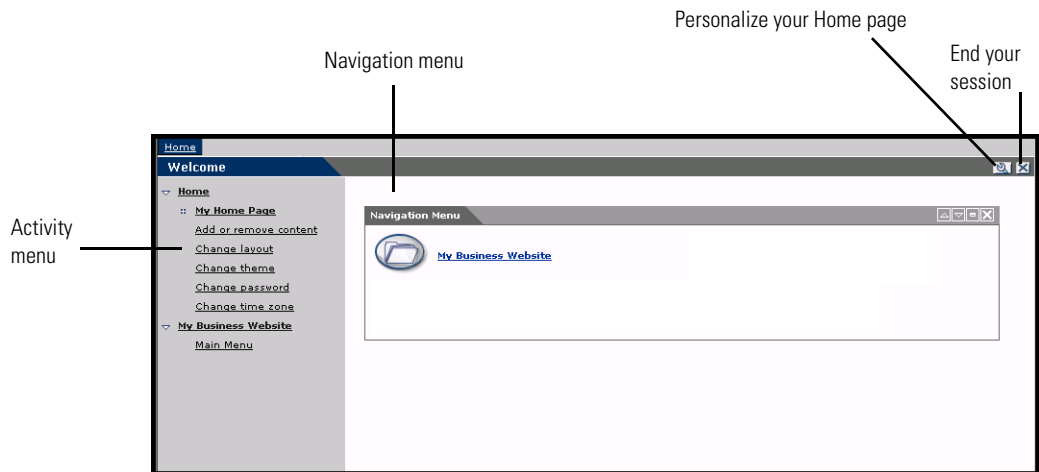


The screenshot shows the user login interface for the Peregrine Portal. The page has a header with the "Peregrine Portal" logo and a "powered by Peregrine" logo. Below the header is a "Login" tab and a "Welcome" message. The main content area contains a login form with the following fields:

- User Name:** A text input field with a search icon to its right.
- Password:** A text input field.
- Language:** A dropdown menu currently set to "English".

Below the form is a "Login" button. The page also includes a "Please enter your user name and password to enter the Peregrine Portal." instruction and a "Login" link in the left sidebar.

The following graphic shows a Portal without any applications installed. The Navigation menu includes modules for your particular application. All applications have the Admin module.



Using the Activity menu

The Activity menu provides access to a number of tasks as you navigate through your Web application. The menu remains visible as you change screens.

The default Activity menu includes the following choices:

Use this option	When you want to
My Home Page	Return to the Peregrine Portal Home page.
Add or remove content	Access the same page as the Personalization button, allowing you to customize your Home page.
Change layout	Change the location of a component or remove it from the Peregrine Portal.
Change theme	Select from several options. Changes take effect immediately after selecting a value in any of these fields. Note: Select the accessible theme to access the alternate text-based interface.
Change time zone	Select the time zone.

Personalizing the Peregrine Portal

By default, the Navigation menu is displayed on the Peregrine Portal. You can personalize the Peregrine Portal to add Get-Answers utilities as well as personal tools such as a calendar, calculator, or the date and time. You can also change the layout of these components or minimize a component to hide the component details.

See the chapter on *Using the Personalization Interface* in this guide for more information on personalization.

Adding components

The following components are available:

Personal Utilities

This component	Provides
Calculator	A tool using standard arithmetic functions.
Calendar	A monthly calendar.
Theme Selector	A drop-down list to change themes.
Date and Time	A date and time display for the local time zone.

Peregrine Portal Web application components

This component	Provides
Navigation Menu	Quick links to the various modules that make up this application.
Document List	A display of a document search, list, or detail screen. Configure the component by choosing the document type you want to expose and the type of screen desired.
My Menu	A menu of links that can be configured dynamically. Links can point to arbitrary web sites, other menus, or document explorer screens.

Note: The Calendar and Calculator require Microsoft Internet Explorer 5.0+ or Netscape 6.1+.

Administration components

Only users with Admin capability have access to the Admin components.

This component	Provides
Connection Status	A list of the adapters currently registered in this server and their connection status.
Control Panel	A button to reset the server and all its connections.
Page Hits / Minute	A list of the total number of pages accessed per minute.
Adapter Transactions / Minute	A list of the number of transactions performed against adapters.
Active User Sessions	A list containing the number of active user sessions.

To add Peregrine Portal components:

- 1 Click the **Personalize** (wrench) icon.

Note: You can also select the **Add or remove content** link from the Activity menu.

The **Customize My Home Page** opens containing a list of the available components.

Customize My Home Page

Here is the type of content that you can include in your home page. Please select the content that interests you. After saving these selections you will be able to customize them to fit your needs.

Personal Utilities

- Calculator** A simple arithmetic adding machine. This component can be viewed using Netscape 6.1, Mozilla .092 and MS Internet Explorer 4.0 or above.
- Calendar** A monthly calendar. This component can be viewed using Netscape 6.1, Mozilla .092 and MS Internet Explorer 4.0 or above.
Change Images, Colors and Styles and Layout.
- Theme Selector**
- Date and Time** Displays date and time for the local time zone or in UTC (Coordinated Universal Time or Greenwich Mean Time) format. This component can be viewed using Netscape 6.1, Mozilla .092 and MS Internet Explorer 4.0 or above.

Peregrine Portal Web Application Components

- Navigation Menu** Quick links to the various modules that make up this application.
Allows the display of a document search, list, or detail screen. Simply configure the component by choosing the document type you want to expose and the type of screen desired.
- Document List**
- My Menu** Presents a menu of links that can be configured dynamically. Links can point to arbitrary web sites, other menus, or document explorer screens.

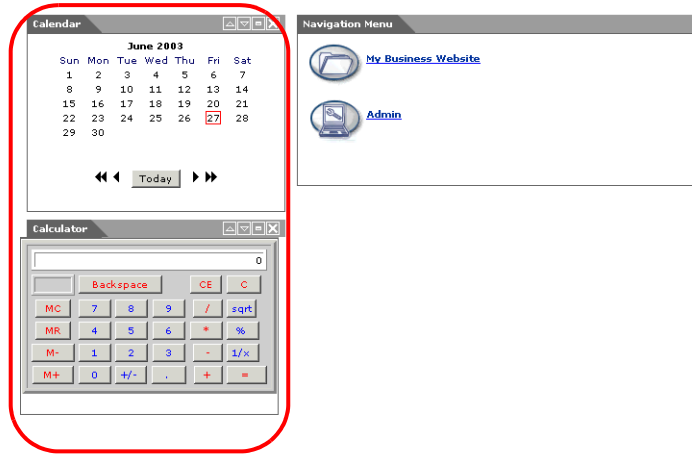
Administration Components

- Connection Status** List of the adapters currently registered in this server and their connection status.
- Control Panel** Reset the server and all its connections.
- Page Hits/Minute** Displays the total number of pages accessed per minute.
- Adapter Transactions/Minute** Displays the number of transactions performed against adapters.
- Active User Sessions** Displays the number of active user sessions.

- 2 Select the components you want to add to your Peregrine Portal.
- 3 When you complete your selections, scroll to the bottom of the page, and then click **Save**. To return to the Peregrine Portal without making any changes, click **Go Back**.

When you return to the Peregrine Portal, the new components are displayed. The following example shows the Calendar and Calculator added to the Portal.

The Calendar and Calculator components display on the Home page after personalization.

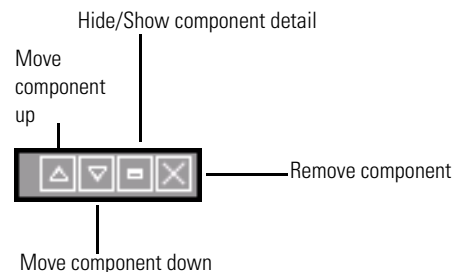


Changing the layout

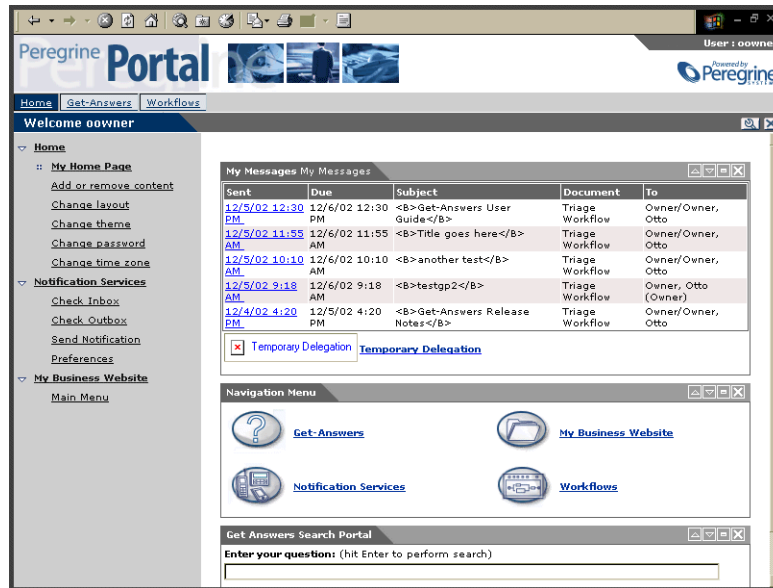
The following sections contain procedures for changing the location of the components or removing them from the Peregrine Portal. The procedure you use is determined by the Web browser you are using.

Microsoft Internet Explorer

If you are using Microsoft Internet Explorer as your Web browser, use the buttons in the upper right corner of each component to move the component up or down, remove the component, or hide/show the component detail.



In the following screen, the Calendar is minimized.

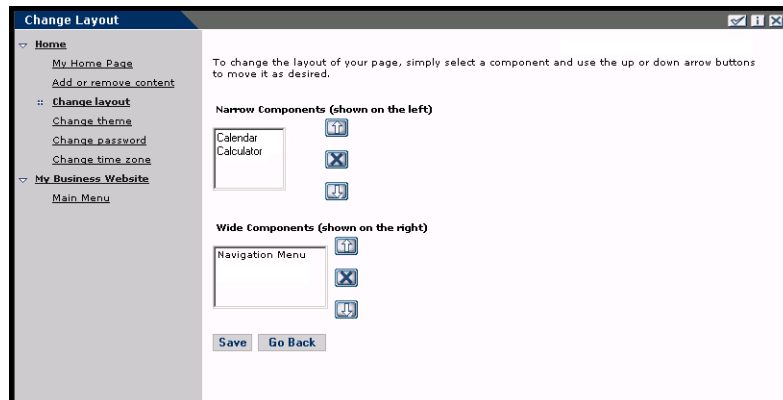


Netscape Navigator

If you are using Netscape Navigator as your Web browser, use the following procedure to change the status of the components on the Peregrine Portal. You can move a component up or down, or remove the component.

- 1 From the Activity menu, select **Change layout**.

A **Change Layout** page opens where you select the components you want to change.



Components can be Narrow (for example, Calendar or Calculator) and are on the left side of the Peregrine Portal. Other components (for example, Navigation Menu) are Wide and are on the right side of the Peregrine Portal.

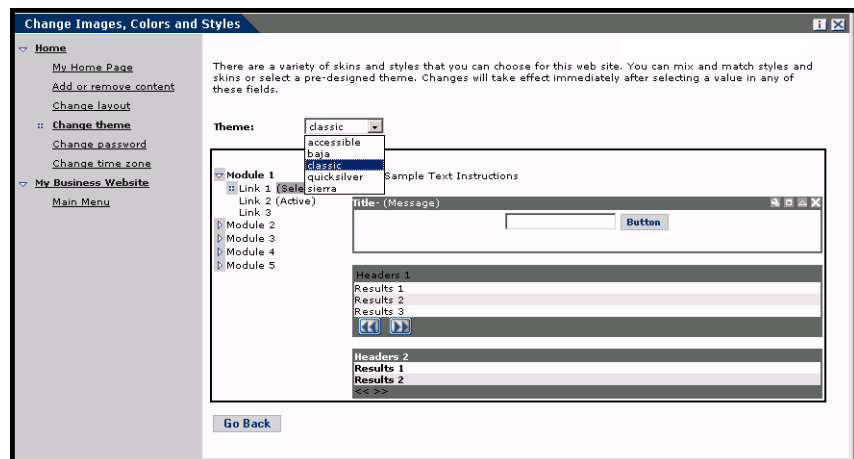
- 2 Select the component you want to modify, and then click the appropriate button to activate the change.
 - Up arrow moves the component up.
 - Down arrow moves the component down.
 - X removes the component from the Peregrine Portal.
- 3 Click Save.

Changing themes

You can choose from a number of themes to change the look of your Web pages. Out of the box, Get-Answers provides five themes you can choose between. If you want to deploy additional themes, refer to *Customizing the Peregrine Portal*.

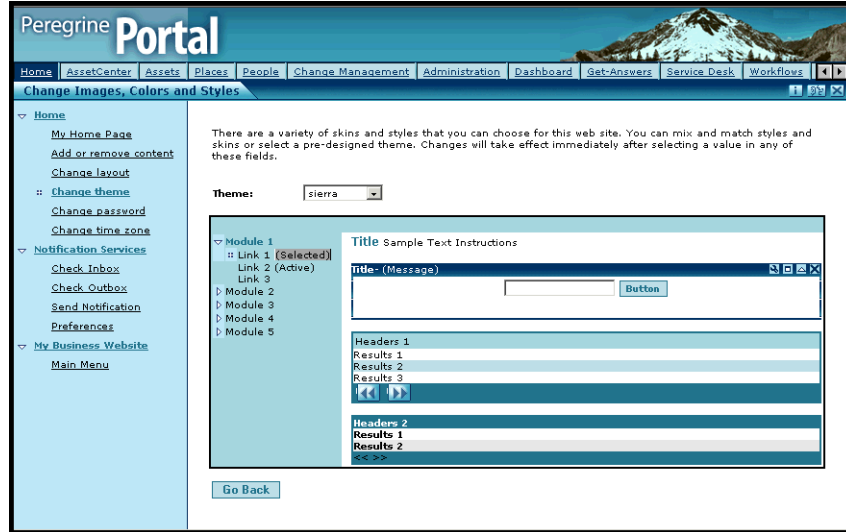
To change the theme:

- 1 From the Activity menu on the Portal Home page, select **Change theme**.
The following page opens.



- 2 Choose from the drop-down list.

As soon as you make your selection, the page updates to reflect your selection. The following example shows the Sierra theme.



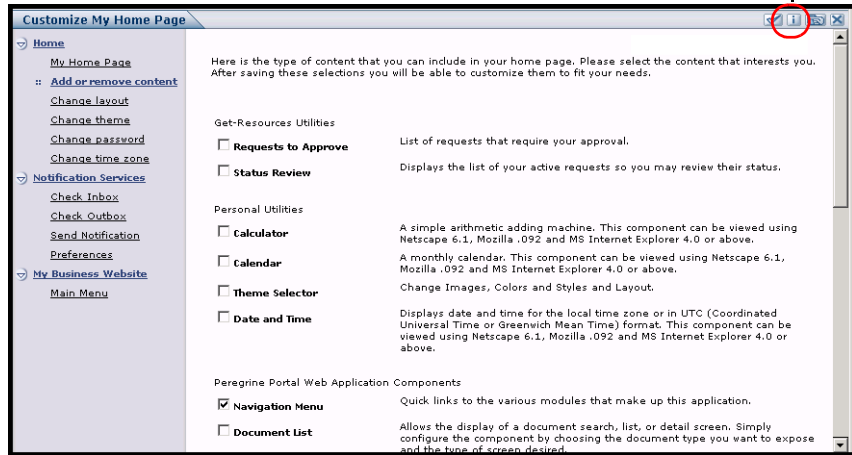
This new configuration remains through subsequent work sessions until changed.

Displaying form information

You can view information about the form you are using. Set this parameter from the Logging tab on the Settings page of the Admin module. See the Get-Answers Administration chapter in this guide for more information.

When the **Show form info** parameter is set to Yes, a **Display Form Info** button appears on the upper right corner of forms.

The Display Form Info button shows information about the form you are using.



4 Customizing the Peregrine Portal

CHAPTER

Peregrine OAA provides a number of ways to customize the interface of an application built on the platform. You can make a quick change, such as replacing the logo with your company logo, or a more complex change such as rewriting the code that defines layer placement or frameset size.

This chapter includes advanced procedures for changing the Peregrine Portal interface. To use this information effectively, you should have knowledge of XML and the CSS2 specifications established by the W3C as outlined at www.w3.org.

Topics in this chapter include:

- *Deploying the Classic theme variations* on page 96
- *Changing the default theme* on page 97
- *Changing the header graphic for all themes* on page 97
- *Creating a custom theme* on page 99
- *Layers properties* on page 103
- *Changing framesets* on page 104
- *Translating Get-Answers* on page 106

Deploying the Classic theme variations

The Classic theme is the default theme that applications built on Peregrine OAA use. It has a gray and teal design and is the theme shown in all the screenshots in the guide. This is the theme you will use to create a customized theme for your enterprise.

There are four variations of the Classic theme:

- *Accessible*, which makes the screen available to users who need high contrast colors or better accessibility support.
- *Baja*, which adds southwestern green and beige hues to the Classic design.
- *Quicksilver*, which adds silver and blue hues to the Classic design.
- *Sierra*, which adds teal hues to the Classic design.

These themes, as well as a number of other optional themes, are deployed with the application installation. Once you create your customized theme, Peregrine Systems recommends that you delete all other themes to prevent users from selecting one of them and overriding your custom theme. If you decide later that you want to manually deploy a theme that has been deleted, or if you did not deploy all themes during the installation, use the following procedure to deploy the themes. The additional themes are zip files located in the `C:\Program Files\Peregrine\oaa\packages` directory. You can identify the theme names from these zip file names.

To deploy an alternate Classic design:

- 1 Open a command prompt window, and change directories to your `oaa\packages` directory. The default path is:
`C:\Program Files\Peregrine\oaa\packages`

- 2 Type:

```
java -jar OAADeploy.jar <name of the theme>
```

Note: List each theme you want to deploy, separated by a space; for example,
`java -jar OAADeploy.jar bluestheme hightechtheme bajatheme.`

- 3 Press ENTER.
- 4 Stop and restart your application server.

The themes you deployed appear as options the next time you log in to Get-Answers.

Changing the default theme

You can change the default theme that all users see when they log in to Get-Answers. Out-of-the-box, the default theme is classic.

To change the default theme:

- 1 Open your Web browser and log in to the Admin module (`localhost/oa/admin.jsp`).
- 2 Click **Settings > Themes**. Change the following parameters:
 - a In the **Default skin/Theme** field, change the parameter to the name of the theme you want to use (for example, *Baja*).
 - b In the **Default stylesheet** field, change the parameter to the appropriate name for the CSS file (for example, *baja.css*).
 - c In the **Default XSL stylesheets** field, change the parameter to the name of the theme you want to use (for example, *Baja*).
- 3 Scroll to the bottom of the page, and then click **Save**.
- 4 When the Control Panel opens, click **Reset Server**.
- 5 Refresh your browser to see the new default theme.

Changing the header graphic for all themes

You can add your corporate logo to all themes in the Peregrine Portal from the Administration Settings page.

Warning: The administration setting discussed below overrides the image used by all themes. If you change this setting then you will see the same logo in all themes. If you want to use a different corporate logo for each theme, see [Creating a custom theme](#) on page 99.

To change the header graphic for all themes:

- 1 Create a custom header graphic.

Note: To fit within the default header frame, your customized header logo must be 514 pixels wide and 59 pixels high. If you want to change the header frame size, see *Changing framesets* on page 104.



- 2 Save your custom header graphic to the following location:

C:\Program Files\Peregrine\Common\Tomcat4\\webapps\oaa\images\skins\classic

Note: The Classic theme is the default theme.

- 3 Log in to the Get-Answers administration page (admin.jsp).
- 4 Click **Settings > Themes**.
- 5 In the **Default Peregrine Portal logo** field, enter the name of your custom header logo.

Portal	Common	Service Desk	Portal DE	Themes	Web Application	Logging	ServiceCenter	XSL	E-mail
Internet Explorer stylesheet path: Directory path for CSS stylesheets for Internet Explorer browser.									
css/									
Images path: Set the images directory location. The directory name must be specified relative to the 'presentation' directory. Setting this allows you to move the default location of the images directory to another location. The default is "images/". You must add the slash at the end of this path.									
images/									
Skins/Themes: Set the Skins directory location. The directory name must be specified relative to the 'presentation' directory. Setting this allows you to move the default location of the skins directory to another location. The default is "skins/". You must add the slash at the end of this path.									
skins/									
Default skin/Theme: Set the Default Skin name for user sessions. Enter only the name of the skin. The default is "classic".									
classic									
Default stylesheet: Set the CSS Stylesheet name for user sessions. To see all the styles used in The Peregrine Portal, click to see the Peregrine Portal Stylesheet Key . This file can be useful for customizing stylesheets. The default is "classic.css".									
classic.css									
Default XSL templates: The default XSL template set to use when the user has not set a theme. This should be the same as the default skin when specifying a theme provided by Peregrine Portal.									
classic									
Default Peregrine Portal logo: Set the global logo to be used in the application. The logo is skinned and is located at the root level of each skin directory in Themes. To add a new custom logo, add it to the skin template. Type in the name for the new logo image. Instructions for adding new images are included in the Peregrine Portal Tailoring Guide. The default logo is "getit_header_logo.gif".									
getit_header_logo.gif									
Application Tab Order: List one module from each of the tab groups in the order that the tabs should appear. Tabs that are omitted will appear at the end of the list in no particular order.									
portal									

Type your new image name.

- 6 Scroll to the bottom of the page, and then click **Save**.
- 7 When the Control Panel opens, click **Reset Server**.
- 8 Refresh the browser to view your changes.

Creating a custom theme

You can create custom themes by copying and modifying the classic theme provided with Get-Answers.

To create a custom theme:

- 1 Copy classic theme images, stylesheets, and XSL templates. These files are located at:
 - Images. `<application server>\oaa\images\skins\classic`
 - Stylesheets. `<application server>\oaa\css\classic`
 - XSL templates. `<application server>\oaa\WEB-INF\templates\classic`
- 2 Paste and then rename the folders for the classic theme to a new name. For example:
 - Images. `<application server>\oaa\images\skins\myTheme`
 - Stylesheets. `<application server>\oaa\css\myTheme`
 - XSL templates. `<application server>\oaa\WEB-INF\templates\myTheme`
- 3 Open and edit each image that you want to change in your new theme. Use the following image conventions.
 - Image file names must remain the same. Get-Answers uses these image names to display theme elements.
 - Image height and width should remain the same unless you are also changing the size of the framesets to accommodate new image sizes.
- 4 Open and edit the `classic.css` file in your new theme.

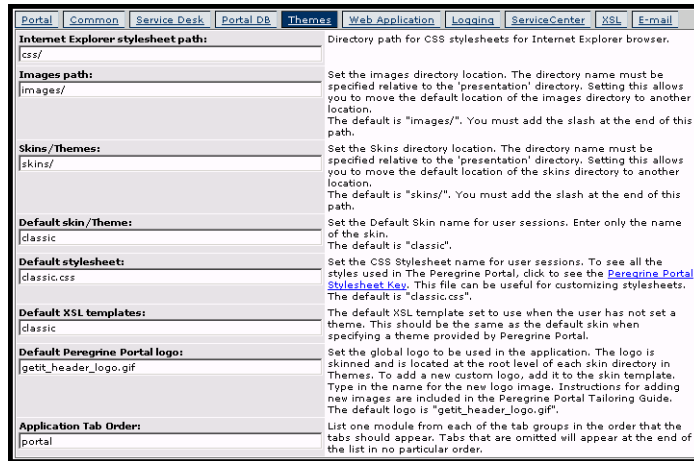
The following table lists some of the more commonly modified styles.

Style Name	Style Description
.ActionButton	The style used on buttons throughout the Portal.
.ActiveMenuLink	Used when the mouse hovers over a menu link.
.ActiveModuleMenu	Designates the currently-selected page within the navigational subset.
.CurrentModuleMenu	Designates the currently-selected navigational subset.
.FormTitle	Used for the title of forms. Normally used to title DocExplorer window content.

Style Name	Style Description
.ListBoxEvenRow	A bolded version of TableEvenRow.
.ListBoxHeading	A bolded version of Table Heading.
.ListBoxOddRow	A bolded version of TableOddRow.
.MenuLink	Used within all module menus.
.ModuleMenu	Used for the left-hand navigational menu.
.ModuleMenuTitle	Designates the navigational subsets title.
.PageTitle	Used on the page title located directly below the logo and tabs.
.TableEvenRow	Used within the table heading with alternating background colors for ease of reading. Has a background color of white.
.TableHeading	Used for application headings for both search and results functions.
.TableOddRow	Used within the table heading with alternating background colors for ease of reading. Has a background color of light gray.
a.ListBoxEvenRow	Designates the style with a link attribute.
a.ListBoxOddRow	Designates the style with a link attribute.
a.TableEvenRow	Designates the style with a link attribute.
a.TableOddRow	Designates the style with a link attribute.

Tip: Modify the style sheets after you complete your overall theme design. Use your image editor's color picker to ensure that the your stylesheet colors match your image colors.

Note: You can see a detailed stylesheet key in the themes Administration section of the Portal. To access the stylesheet key, locate the Default stylesheet field on the Themes tab of the Admin Settings page and click the [Peregrine Portal Stylesheet Key](#) link.



- 5 Save your theme stylesheet with the same name as your new theme. For example, `<application server>\oaa\css\myTheme\myTheme.css`.
- 6 Open and edit the `layers_<xx>.jsp` file to change any layer descriptions. To change layers for Internet Explorer, open `layers_ie.jsp`. To change layers for Netscape open `layers_gecko.jsp` extension. For more information about editing layers see [Layers properties](#) on page 103.
- 7 Open and edit any XSL stylesheets you want to change.

Warning: Do not change these files unless you have knowledge of XSL and HTML transformation.

The XSL stylesheets determine how Get-Answers displays form components in the main portal frame.

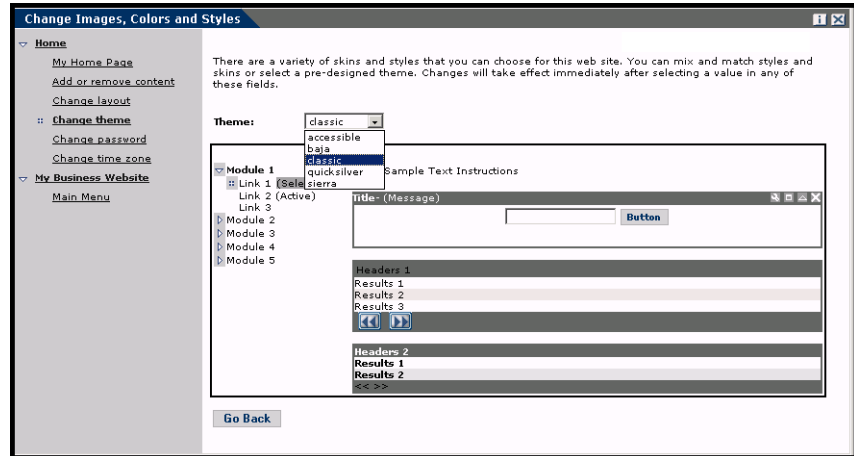
The following table lists the XSL stylesheets you can change.

To change	edit this XSL stylesheet
Attachment picker	attachments.xml
HTML form generation	basic-form.xml

To change	edit this XSL stylesheet
Action (button) properties	button.xsl
Template components	components.xsl
Debugging message properties	copy_nodes.xsl
Date-time picker properties	datetime.xsl
Text edit field properties	edit_fields.xsl
Entry table form component (see administration page for examples)	entrytable.xsl
Field section properties	fieldsection.xsl
Field table properties	fieldtable.xsl
HTML page generation	form.xsl
Frameset properties	frames.xsl
Images properties	image_fields.xsl
Label properties	labels.xsl
Link properties	link.xsl
Building of DocExplorer lists	list-builder.xsl
Lookup field properties	lookup_fields.xsl
Money text field properties	money_fields.xsl
Portal properties	portal.xsl
Radio checkbox properties	radio_checkbox_fields.xsl
Read-only text field properties	readonly_fields.xsl
Select text field properties	select_fields.xsl
Spinner properties	spinner_fields.xsl
SVG image properties	svg_cad.xsl
Table properties	table.xsl
Navigation tab properties	tabs.xsl

- 8 Stop and restart your application server.

You can view your new theme by selecting it from the *Change theme* page, available from the Peregrine Portal Home page.



Layers properties

The following sections describe the `layers_ie.jsp` and `layers_gecko.jsp` files. Each layer is defined by a separate `<div>` tag entry and includes an `id` attribute that names the layer. You can change layer properties as needed, but the following layers are required and should not be removed:

- logo

```
<div id="logo" style="position:absolute; left: 0px; top: 0px; width:
100%; height: 40px; z-index: 3;">

</div>
```

- time

```
<div id="time" style="position:absolute; right: 4px; top: 84px;
width: 100%; z-index: 13;" onmouseover="_pauseAlert()"
onmouseout="_startAlert()" class="userBarText">
</div>
```

- toolbar

```
<div id="toolbar" style="position:absolute; width: 50px; top: 59px;
right: 0px; z-index: 12;"></div>
```

- user

```

<div id="user" style="position:absolute; top: -4px; right: 0px;
z-index: 14;">
<table width="100%" border="0" cellpadding="0" cellspacing="0"
align="right">
<tr>
<td width="50%">&nbsp;  </td>
<td nowrap width="3" align="right" valign="top">
">
</td>
<td nowrap align="right" valign="top" width="100%" background="<%=
Archway.getSkinImagePath("backgrounds/rt_tile.gif", user ) %>">
">
</td>
<td nowrap><font class="userBarText" size="1" face="Arial, Helvetica,
sans-serif"><%=userTitle%></font>&nbsp;  &nbsp; </td>
</tr>
</table>
</div>

```

■ tabs

```

<div id="tabs" style="position:absolute; left: 0px; top: 60px; width:
100%; z-index: 11;" >
</div>

```

■ form titles

```

<div id="formTitles" style="position:absolute; left: 10px; top: 81px;
width: 200px; z-index: 16;">&nbsp;  
</div>

```

Changing framesets

Important: You must have advanced knowledge of HTML, JSP, and framesets to modify these files. Keep all of the frames and do not change the names of any of the frames. Doing so will result in JavaScript errors.

There are two framesets to be modified for each browser. These files are in C:\Program Files\Peregrine\Common\Tomcat4\webapps\oaa\images\skins*<your theme>*.

The `frames_xx.jsp` files are for the pages that you access when logging in as an end-user (`login.jsp`). The `admin_frames_xx.jsp` files contain the configuration for the Admin module (accessed when you log in using `admin.jsp`).

To change framesets:

- 1 Stop your application server.
- 2 Open the browser-specific frameset file `frames_<xx>.jsp` in a text editor (where `<xx>` is `ie` for Internet Explorer and `gecko` for Netscape).
- 3 Modify the frameset properties.
- 4 Save the file.
- 5 Restart your application server.

You can now test your changes in your Web browser.

The following sections show the complete `_ie.jsp` files as examples of the frameset files.

`frames_ie.jsp`

```
<%@ include file="../../../jspheader_2.jsp" %>
<%@ include file="../../../message_special.jsp" %>

<frameset onload="setTopFrames()" onunload="closeChildWindows()"
border="0" framespacing="0" frameborder="NO" cols="*" rows="102,*">
  <frame scrolling="NO" marginwidth="0" marginheight="0"
src="oaa_header.jsp" name="getit_main_head">
    <frameset cols="185,10,*" rows="*" frameborder="no" border="0"
framespacing="0">
      <frame scrolling="AUTO" marginwidth="0" marginheight="0"
src="apphead.jsp" name="getit_header">
        <frame name="framesep" scrolling="no" marginheight="0"
marginwidth="0" src="framesep.jsp">
          <frameset rows="*,0">
            <frame scrolling="AUTO" marginwidth="6" marginheight="6"
src="e_login_main_start.jsp?<%= user.getADW(msg,"Params" ) %>"
name="getit_main">
              <frame noresize scrolling="NO" marginwidth="0"
marginheight="0" src="backchannel.htm" name="backchannel">
            </frameset>
          </frameset>
        </frameset>
      </frameset>
    </frameset>
```

`admin_frames_ie.jsp`

```
<%@ include file="../../../jspheader_2.jsp" %>
<%@ include file="../../../message_special.jsp" %>
```

```

<frameset onload="setTopFrames()" onunload="closeChildWindows()"
border="0" framespacing="0" frameborder="NO" cols="*" rows="102,*">
  <frame scrolling="NO" marginwidth="0" marginheight="0"
src="aaa_header.jsp" name="getit_main_head">
    <frameset cols="185,10,*" rows="*" frameborder="no" border="0"
framespacing="0">
      <frame scrolling="AUTO" marginwidth="0" marginheight="0"
src="apphead.jsp" name="getit_header">
        <frame name="framesep" scrolling="no" marginheight="0"
marginwidth="0" src="framesep.jsp">
          <frameset rows="*,0">
            <frame scrolling="AUTO" marginwidth="6" marginheight="6"
src="e_adminlogin_login_start.jsp?<%= user.getADW(msg, "Params") %>"
name="getit_main">
              <frame noresize scrolling="NO" marginwidth="0"
marginheight="0" src="backchannel.htm" name="backchannel">
            </frameset>
          </frameset>
        </frameset>
      </frameset>
    </frameset>
  </frameset>

```

Translating Get-Answers

Out-of-box, all Peregrine OAA web applications are provided in English. You can order translated versions of the core Peregrine OAA web applications by purchasing a language pack. Peregrine OAA 4.1 language packs will be available in September, 2003 for the following languages:

- French
- Italian
- German

Note: Not all Peregrine OAA web applications will offer language packs. Refer to the Peregrine support web site to determine the availability of language packs for your Peregrine OAA web applications.

If you have a language pack version of a Peregrine OAA web application, you will need to edit the existing string files for these applications and add any new strings that resulted from your tailoring efforts. For more information on the process, refer to *Editing existing translation strings files* on page 107.

If you do not have a language pack version of your Peregrine OAA web applications and you want to create a new translation, refer to the instructions in *Adding new translation strings files* on page 107.

To configure the Peregrine OAA Platform to use your new translation, see *To configure the Peregrine OAA Platform to use new string files*: on page 108.

Editing existing translation strings files

You can make edits, additions, and deletions to string files outside of Peregrine Studio using any text editor or standard translation software.

To edit an existing translation string file:

- 1 Open the translated string file in a text editor or translation program.
You can find all the translation string files in your application server's installation directory:

```
<application server>\oaa\WEB-INF\apps\<group of modules name>
```

Note: The string file will use the ISO-639 two letter abbreviation for the language in the file name.

- 2 Search for an existing string that you want to change.

The string file uses the format illustrated below:

```
String_label, "translated string"
```

Where *String_label* is a unique name given to the string, and

Where *translated string* is the actual value of the string to be translated.

For example if you added a new button, you might look for:

```
EMPLOOKUP_EMPLOYEELOOKUP_SEARCH_LABEL, "Search"
```

- 3 Change the “*translated string*” portion of the new string to the target language of your translation. For example, to change the string listed above to French, you might enter the following:

```
EMPLOOKUP_EMPLOYEELOOKUP_SEARCH_LABEL, "Recherche"
```

- 4 Save the new string file.

The new translation strings will be available as soon as you stop and restart the application server.

Adding new translation strings files

You can add new string files to the Peregrine OAA Platform to provide additional language support to your Get-It web applications. The translation process can be accomplished using any text editor or standard translation software.

Important: Peregrine does not support Get-It web applications translated into any languages other than those listed in *Translating Get-Answers* on page 106.

To add an existing translation string file:

- 1 Open the English string file for your Studio project in a text editor or translation program.

You can find all the translation string files in your application server's installation directory:

```
<application server>\oaa\WEB-INF\strings
```

Note: The English string file will have the ISO-639 two letter abbreviation EN in the file name.

- 2 Copy the entire the English string file.
- 3 Create a new string file for the target language in which you want to add a translation.

Note: The string file must use the ISO two letter abbreviation for the language in the file name.

- 4 Paste the copied English string file into the new file.
- 5 Change the “*translated string*” portion of each string to the target language of your translation.
- 6 Save the new string file.

The new translation strings will be available as soon as you stop and restart the application server.

To configure the Peregrine OAA Platform to use new string files:

- 1 Log in as an administrator (the administrator login page is located at `admin.jsp`).
- 2 Click **Settings**.
- 3 Click the **Common** tab.
- 4 Enter the two letter ISO-639 language code for the languages you want to support in the **Locales** field. The first code entered will be the default language used. The other languages you define will be available in a drop-down list.

- 5 In the **Content type encoding** field, enter the character encoding to be used for the display language. The following table lists some of the common character encoding formats.

Character Encoding	Character Set
ISO-8859-1	U.S. and Western European character sets. This is the default character set used by Studio.
Shift_JIS	Japanese character set
ISO-8859-2	Polish and Czech character set

- 6 Click **Save** at the bottom of the Settings form to save your changes.
- 7 On the Console form, click **Reset Server** to implement your changes.
Users will now be able to select the display language for their session used when they login to the Peregrine OAA Platform.

5 Personalization

CHAPTER

Personalization is available to both administrators and end users in Peregrine Systems Web applications built using Document Explorers (Doc Explorers). Authorized users can change the appearance and functionality of certain Web applications directly from the application interface.

With a Personalization interface, users can add or remove fields, rearrange how fields are displayed, or add, change, or delete records from a back-end database.

This section includes:

- *Personalization overview* on page 112
- *Supporting personalization* on page 115
- *Personalization tasks* on page 118
- *Moving Personalizations from a development to a production environment* on page 123

Personalization overview

Personalization allows end users a means to create and customize searches of Get-Answers data. From the end-user perspective, personalization is a collection of standard forms that allow users to change part of the interface to suit their needs. The administrator determines which forms and features of personalization each user has by setting global personalization rights and by granting individual users capability words to do additional personalization.

From the administrator's perspective, personalization is a customization option that allows users to change the Get-Answers interface without the need to rebuild a Peregrine Studio project for every change made. Personalization enables users to add or remove fields, change the layout of a form, and change interface elements such as headers and buttons in real time using the browser interface.

Forms and functions

Personalization is based on a collection of forms collectively referred to as a DocExplorer. Doc Explorer forms provide the following functionality:

- A search form for defining search criteria.
- A list form for displaying search results.
- A details form for displaying detailed information about search results.

If you grant end-users administrative rights, they can also use Personalization for the following actions:

- Add a new record to the database from a creation form.
- Update existing records in the database from the detail form.
- Delete existing records from the database from the detail form.

Personalization interface



You can personalize any Web application interface that displays a wrench icon in the top right of the interface frame. The wrench icon will appear only in activities where a Personalization form has been defined. The Personalization form determines what options are displayed in the Personalization pop-up window.

When you click on the Personalization icon, a pop-up window opens displaying the current settings for the form you are viewing.

The Available Fields column contains all the fields that can be added to a form.

The Current Configuration column contains the fields that currently visible on the form.

Select the fields you want to display when examining a **Ticket** document. Double click on a field in the right column to edit its attributes.

Document Fields	Current Configuration
Available Fields	Current Configuration
-- Left/Right Split --	-- Ticket Details --
-- Top/Bottom Split --	Ticket Number
-- Section Title --	Status
Asset Tag	Category
Assignment Group	Severity
Attachments	Priority
Category	Opened By
Cause Code	Open Time
Company Id	-- Top/Bottom Split --
Contact Name	-- Description --
Description	Description

Form Options

Title:

Instructions:

Explorer Options

Create: Go directly to the create screen by default

Skip search: Skip the search page and execute a default query

Single Detail: Go directly to detail page when search finds exactly one item

Summary: Show a summary page for the document

Restrict operations to the following roles:

Document Creation:

Document Deletion:

Document Update:







Administrators determine what available data fields display on each form. The wrench icon only appears in activities where a Personalization form has been defined. The Personalization form determines what options display in the Personalization pop-up window.

When you click on the Personalization icon, a pop-up window opens displaying the current settings for the form you are viewing. All Personalization pop-up windows have the following format.

Field	Description
Available Fields	Shows all the document fields and subdocument collections that can be added to the current form. Peregrine OAA generates the list of available fields by dynamically reading the schema that the form uses. Any items listed between dashes are form components you can use to organize and arrange how document fields are displayed in the form.
Current Configuration	Shows all the document fields, subdocument collections, and displays components that are on the current form.
Form Options Title Instructions	Defines the form name and specific instructions to follow when using the form.
Explorer Options Create Skip search Single Detail Summary	Defines how Peregrine OAA displays results. Users only see the Options section if they have administrative Personalization rights.
Restrict operations to the following roles Document Creation Document Deletion Document Update	Determines whether users can update, create, or delete records from the back-end database system. Users only see the Restrict section if they have administrative Personalization rights.
Revert to Default	Removes all Personalization entered by the end user and returns the form to the default state as determined by the Get-Answers administrator or the form's schema.
Save	Saves and applies your Personalization changes to the current form.

Personalization icons

You personalize the Get-Answers pages by adding, moving, and removing fields. Select the page you want to personalize, then select the fields you want to display on the screen.

Icon	Description
	The Personalize (wrench) icon allows you to edit any attributes available for the field. Not all components contain the edit option. Press Save at the bottom of the page to save your changes.
 	The Move (vertical arrows) icons move the component either up or down on the page. Moving components is always performed with these arrows.
	The Plus (+) icon adds a component to your current configuration.
	The Insert icon adds a component in the specified place on the screen.
	The Remove (X) icon removes the component from the page. Removing a component does not delete the component; it only does not display it.

Supporting personalization

To support Personalization, you must have these components:

- An AssetCenter or ServiceCenter back-end database. Personalization requires you to store users' login rights and Personalization changes in one of these two databases.
- Adapter aliases defined for the following tabs on the Get-Answers Administration settings page:
 - Portal
 - PortalDB
 - Web Application

Activating Personalization

Personalization is intended to be an administration tool. Administrators can add and remove the fields they want to display in the interface and then turn off personalization to prevent end-users from adding or removing fields.

If end-users have personalization access, there is no way to prevent them from changing fields available through personalization.

You can grant users access to personalization features in one of two ways:

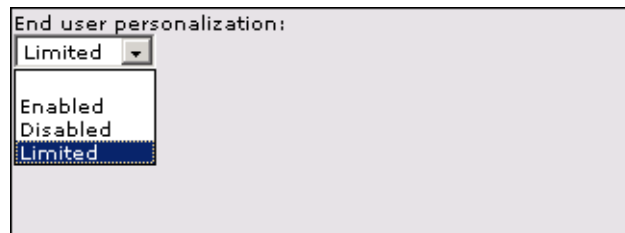
- Grant all users personalization rights by setting the end-user personalization administrative setting.
- Grant individual users personalization rights by adding a capability word to their user profile.

Granting global personalization rights

You can globally define end-user access to personalization by selecting one of three options from the End User Personalization options.

To grant all users personalization rights:

- 1 Login to the Get-Answers administration page.
- 2 Click **Administration > Settings**.
- 3 Click the **Common** tab and scroll down to the **End user personalization** parameter.
- 4 Select the level of personalization you want to grant all users from the **End user personalization** drop-down list.



- **Enabled.** This setting grants all users the `getit.personalization.default` capability word, which enables end-users to add or remove any field listed in the schema used by a DocExplorer. However, only end-users who also have the `getit.personalization.admin` (or equivalent) capability word will be able to use the advanced explorer options.

- **Disabled.** This setting globally turns off all personalization except to users who the administrator has granted individual personalization rights by adding a capability word to their user profile in the Get-Answers back-end database. The personalization wrench icon will be hidden from the Get-Answers interface, and any end-users who have individual personalization rights will only see the fields that an administrator has configured to be visible.
 - **Limited.** This setting grants all users the `getit.personalization.limited` capability word, which enables end-users to add or remove only the fields that appear on a form by default or that administrator has made visible. Unless end-users have an individual capability word with greater rights, end-users can only add or remove the fields that an administrator has configured to be visible. This setting also prevents end-users from changing read-only fields to editable fields.
- Tip:** Peregrine Systems recommends that personalization be restricted to administrators in the production environment. That is, set the global Personalization setting to **Disabled** and then add the capability word `getit.personalization.admin` to the administrative user.

Granting individual personalization rights

You can grant individual users personalization rights by adding a capability word to the user profile stored in the Get-Answers back-end database. The following personalization capabilities words are available:

- `getit.personalization.limited`—Users can only personalize features that have been exposed by a user with greater personalization rights.
- `getit.personalization.default`—Users can change the layout and add or remove fields from the Get-Answers interface.
- `getit.personalization.admin`—Users can do everything that the default capability word allows plus users can set personalization options and save personalization changes as the default layout. The admin capability word also grants the following rights:
 - **Document Creation.** Users can specify the capability words required to create new records in the back-end database.
 - **Document Update.** Users can specify the capability words required to submit records to the back-end database.
 - **Document Deletion.** Users can specify the capability words required to delete records from the back-end database.

- Save. Any personalization changes that the admin user saves determine what other users see. If the admin user adds a field, then the field becomes visible in the available fields list for other users. If the admin user removes a field, then the field is hidden from other users.

By default, users have no personalization capability word. To add a capability word, you must add it to the Get-Answers back-end database or set global personalization rights.

Personalization tasks

Using DocExplorer, you can personalize any Web application interface that has a wrench icon in the top right of the Peregrine OAA frame. DocExplorers allow end users a means to create and customize searches of data. From the end-user perspective, a DocExplorer is a special activity that allows someone to personalize part of the interface. The user's profile determines the Personalization rights granted.

Adding fields to a form

With personalization rights, you can add fields to a form from the Available Fields list. You can then change the layout, if needed. Your personalization rights determine the lists of fields that you see.

You can add a field that is not currently available in the DocExplorer's schema by creating a schema extension. See the *Document Schema Definitions* chapter in this guide for more information on adding a new field.

Note: Data is not displayed in newly added DocExplorer fields. Users must close and resubmit the search or detail query before data will appear in a new DocExplorer field.

To add fields to a form:

- 1 Do one of the following:
 - From the upper right corner of the active form, click the **Personalize** icon.
 - From the lookup page, click **Personalize this page**.
- 2 Select a field from the **Available Fields** list.
- 3 Click the **Plus (+)** icon.
The field appears in the Current Configuration list.
- 4 Optionally, click the **Insert** icon to insert a component.

5 Click **Save**.

Tip: The browser warns that data must be present when adding fields in DocExplorer. Click **Retry** to resend the data to the browser. This is expected behavior of DocExplorer.

To arrange the field order:

- 1 Select a field from the **Current Configuration** list.
- 2 Click the up arrow or down arrow to change the field's position in the **Current Configuration** list.
- 3 Click **Save**.

To change the field layout:

- 1 From the **Available Fields** list, select **Left/Right Split**.
- 2 Click the **Plus (+)** icon.

To add a new section:

- 1 From the **Available Fields** list, select **Section Title**.
- 2 Click the **Plus (+)** icon.

Note: See *Changing the label of a field* on page 121 for information on editing the **Section Title** field.

- 3 From the **Current Configuration** column, arrange the order of the section with the **Up**, **Down**, and **Remove** icons.

Note: These icons either move or delete a field. Deleting a field removes the item from the form.

- 4 Click **Save** to keep your changes and return to the form.

Configuring field attributes

Each field in a personalization form has its own set of attributes that you can modify. Depending on your personalization rights, you can rename the field label (see page 121), change the field to read-only (see page 121), require users to enter a value (see page 122), and change the size and span of a field (see page 122).

[Project.studio.personalize.attribute.start](#) 

Please change any of the following attributes so that it is presented to meet your exact needs.

cols:
colspan:
default:
label:
readonly: Yes No
required: Yes No
rows:
rowspan:
size:

To configure field attributes:

- 1 Double click a field from the **Current Configuration** list to open an edit window.
- 2 Enter the new field attributes.

Note: Each field has its own set of field attributes. The following table only lists the more common field attributes:

Field	Description
Colspan	The number of data cells in a column.
Label	The name to be used as the field label. This name appears next to the field in the Get-Answers interface.
Readonly	Yes prevents users from updating information displayed in the field.
Required	Yes requires the field to have a value before the form can be submitted.

Field	Description
Rowspan	The number of data cells in a row.
Size	The number measurement of a component in a cell.

- 3 Click **Save** to save your changes and return to the previous pages.
Cancel returns you to the previous page without saving your changes.

Changing the label of a field

To change the existing label of a field, you must have personalization rights.

To change the label of a field:

- 1 From the **Current Configuration** column, select the label you want to change.
- 2 Click the **Personalize** (wrench) icon.
The Personalization window opens.
- 3 Type the new name in the **Label** text box, then click **Save** to save your changes and return to the previous pages.
Cancel returns you to the previous page without saving your changes.

Changing a field to read-only

You can make a field read-only if you do not want users updating information in the displayed field.

To change a field to read-only:

- 1 From the **Current Configuration** column, select the field you want to be read-only.
- 2 Click the **Personalize** (wrench) icon.
The Personalization window opens.
- 3 Toggle the **Read Only** field to **Yes**.
- 4 Click **Save** to save your changes and return to the previous pages.
Cancel returns you to the previous page without saving your changes.

Making a field required

You can require users to enter a value in a field before they can submit a form.

To make a field required:

- 1 From the **Current Configuration** column, select the field you want to be required.
- 2 Click the **Personalize** (wrench) icon.
The Personalization window opens.
- 3 Toggle the **Required** field to **Yes**.
- 4 Click **Save** to save your changes and return to the previous pages.
Cancel returns you to the previous page without saving your changes.

Changing the size and span of a field

You can change the dimensions of the field by assigning values to the row span and size.

To change the size and span of a field:

- 1 From the **Current Configuration** column, select the field you want to change.
- 2 Click the **Personalize** (wrench) icon.
The Personalization window opens.
- 3 Type the values for the **Row Span** and **Size**.
- 4 Click **Save** to save your changes and return to the previous pages.
Cancel returns you to the previous page without saving your changes.

Removing fields from a form

To remove fields from a form:

- 1 Select a field from the **Current Configuration** list.
- 2 Click the **X** button to remove the field.
- 3 Click **Save**.

Moving Personalizations from a development to a production environment

You can easily export personalizations that you created in a development environment and import them to a production environment. Moving the files is a two-step process:

Step 1 Export the personalization files from your development environment.

Step 2 Import the personalization files to your production environment.

To export personalization files:

- 1 Login to the development application server Administration page.
- 2 Click **Admin > Import/Export**.
- 3 Type the path to an existing folder on the server, including a file name, to make the file available to the production server.
- 4 Click **Export**.
- 5 Manually copy the file from your development server to your production application server.

To import personalization files:

- 1 Login to the production application server Administration page.
- 2 Click **Admin > Import/Export**.
- 3 Change the path and file name to the path and file name of the file you want to import.
- 4 Click **Import**.

6 Schemas

CHAPTER

This document describes document schema definitions and explains how they map data between Get-Answers and the back-end database. In addition, this document discusses how to use schema extensions to add new logical and physical mappings to the KmDocument schema.

This document covers the following topics:

- *Understanding Document Schema Definitions* on page 126
- *How to use schemas* on page 127
- *Schema extensions* on page 128
- *Editing the schema extension files* on page 131
- *Schema Elements and Attributes* on page 136

Understanding Document Schema Definitions

A document schema definition (also called a schema) is an XML file that instructs the Archway Document Manager how to query back-end databases and generate XML documents containing the query response. Schemas are mapping tools that determine which XML tags used in dynamically created documents map to the table and field names in a given back-end database. These generated XML documents provide the data that Get-Answers displays and processes.

All schemas consist of two types of definitions:

- **Base definitions**—The schema entries that provide a logical mapping between the XML tags generated in a document query to the Get-Answers interface are collectively referred to as the schema base definitions. The Archway Document Manager uses the base definitions to generate XML tags based on the elements listed in the schema. The Archway Document Manager converts the name value listed in an <attribute> element into a XML tag of the same name.
- **Derived definitions**—The schema entries that provide a physical mapping between the XML tags generated in a document query to the table and field names in the back-end database are collectively referred to as the schema derived definitions. The Archway Document Manager queries the tables and field names listed in the schema and creates an XML document with the results of the query. The Archway Document Manager converts the table and field values listed in the <document> and <attribute> elements into a SQL query.

Note: The document schema definitions used by Peregrine Studio are not the same as the schemas being proposed and developed by the W3C.

The base and derived definitions each have their own list of legal elements and attributes. For more information on schema elements and attributes and how to use them, refer to *Schema Elements and Attributes* on page 136.

How to use schemas

In most cases, you access a schema through personalization where the list of available fields for personalization is determined by the schema. For more information about how to use personalization, refer to the *Personalization* chapter of this guide. If you want to change the fields that are available through personalization, you can create a schema extension.

A schema extension is a separate file listing only the changes you make to an existing schema's logical or physical mappings. For example, you could create a schema extension to provide updated physical mappings when you upgrade your back-end database. Creating schema extensions is the preferred method of tailoring schemas as your changes are stored in separate files that can be easily carried over during an upgrade.

Schema extensions

You can create schema extensions to add new *logical* and *physical* mappings to your existing schemas. Schema extensions allow you to save any additional mappings in separate files that preserve the original schema files shipped by Peregrine Systems. This separate file organization ensures that any upgrades will not overwrite your tailoring changes.

Sample schema

The following is a sample schemas that you can use as a template for your schema extension logical and physical mappings for the rKmDocument schema.

The file

```
C:\ProgramFiles\Peregrine\Common\Tomcat4\webapps\  
oaa\WEB-INF\apps\oaagen\schema\extensions\rKmDocument.xml
```

lists the schema extension mappings.

```
<?xml version="1.0" encoding="UTF-8"?>  
<schema>  
  <documents name="rome">  
    <document name="rKmDocument">  
      <attribute label="Product" name="Product" type="number"/>  
      <attribute label="Solution" name="Solution" type="number">  
        usertype="jsp:rtf_field.jsp"/>  
    </document>  
  </documents>  
  <documents name="rome">  
    <attribute field="_null" member="Product" name="Product"/>  
    <attribute field="_null" member="Solution" name="Solution"/>  
  </documents>  
</schema>
```


When to use schema extensions

Schema extensions generally provide the most benefit when you use them to extend existing schemas. Extending a schema allows you to do the following tailoring tasks without the need to rebuild a project in Peregrine Studio:

- Add new fields to the Available Fields list.
- Hide existing fields from the Available Fields list.
- Change the label that a field displays in the Available Fields list.
- Change the list of forms where a field displays.
- Change the physical mapping of a field.
- Change the type of data a field stores.

Extending schema extensions in Get-Answers

You can create schema extensions using any Text editor to extend the KmDocument schema in Get-Answers. In a typical installation, it is located at:

```
C:\Program Files\Peregrine\Common\Tomcat4\webapps\oaa\WEB-INF\apps\oaagen\schema\extensions
```

The Get-Answers Importer creates your schema extension files for you. If you have legacy documents to import, see [Chapter 11, Importing Legacy Data](#), which explains how to use the Get-Answers Import Documents feature. This is the feature that creates the KmDocument schema extension for you.

The KmDocument schema extension is located in the following subfolder on a typical installation:

```
C:\Program Files\Peregrine\Common\Tomcat4\webapps\oaa\WEB-INF\apps\oaagen\schema\extensions
```

- Schema extension logical and physical mappings. This file contains the schema base and derived definitions. You or the Document Importer create this file in a subfolder of schema called extensions, and it has the same name rKmDocument.xml:
schema\extensions\rKmDocument.xml

To create the schema extension target folders and files yourself:

Copy the sample schema XML source file into the following directory:

C:\Program Files\Peregrine\Common\Tomcat4\webapps\oaa\WEB-INF\
apps\oaagen\schema\extensions

```
<?xml version="1.0" encoding="UTF-8"?>
<schema>
  <documents name="rome">
    <document name="rKmDocument">
      <attribute label="Product" name="Product" type="number"/>
      <attribute label="Solution" name="Solution" type="number">
        usertype="jsp:rtf_field.jsp"/>
    </document>
  </documents>
  <documents name="rome">
    <attribute field="_null" member="Product" name="Product"/>
    <attribute field="_null" member="Solution" name="Solution"/>
  </documents>
</schema>
```

Editing the schema extension files

The edits that you need to do to the schema extension files depend upon what features you are trying to include. The following sections outline what edits you need to perform for each feature.

- *Adding a new field to the Available Fields list* on page 131.
- *Hiding an existing field from the Available Fields list* on page 132.
- *Changing the label a field displays in the Available Fields list* on page 133.
- *Changing the list of forms where a field is available or visible* on page 133.
- *Changing the physical mapping of a field* on page 134.
- *Schema Elements and Attributes* on page 136.

Adding a new field to the Available Fields list

You can add a field to any form that uses personalization. New fields display as options in the personalization Available Fields list.

To add a new field to Available Fields list:

- 1 Open the schema extension file in the extension folder.
This file is for your schema extension logical and physical mappings.
- 2 In the upper `<documents>` section, add a logical mapping `<attribute>` element for each field you want to add to the list of Available Fields.

You must add each `<attribute>` element between the `<document>` tags:

Add new logical mappings here

```
<documents name="rome">
  <document name="rKmDocument">
    <attribute label="Product" name="Product" type="number"/>
    <attribute label="Solution" name="Solution" type="number"
      usertype="jsp:rtf_field.jsp"/>
  </document>
</documents>
```

- a Add the required name and type attributes to each `<attribute>` element.
- b Add any optional attributes you want to use for each `<attribute>` element.
- c Add `usertype="jsp:rtf_field.jsp"` if the field is a rich text field (RTF) field. The Solution field above is an example of this.

Refer to `<attribute>` on page 140 for additional information on the `<attribute>` element.

- For each logical attribute in the upper `<documents>` section, add an `<attribute>` element between the `<document>` tags for the physical attribute in the lower `<documents>` section.

Add new physical mappings here

```
<documents name="rome">
  <document name="rKmDocument">
    <attribute field="_null" member="Product" name="Product"/>
    <attribute field="_null" member="Solution" name="Solution"/>
  </document>
</documents>
```

- Add the required name, member, and field attributes for each entry you defined in the logical mapping. In the example, `field="_null"` is required to tell the rome adapter that there is no separate physical mapping for this field in the database, which means that this field does not have its own column in the KmDocument table. Instead, it is packaged into the DocBody blob column in the KmDocument table along with other fields marked with `_null`. The `member` field is used by the rome adapter and must have the same value as the `name` field.
 - Add any optional attributes you want to use for the physical mapping. See *<attribute>* on page 140 for more information on optional attributes of the `<attribute>` element.
- Save the schema extension file.

Hiding an existing field from the Available Fields list

You can hide a field from the list of Available Fields in personalized forms. Hidden fields will not be available to any user regardless of user rights.

To hide an existing field from the Available Fields list:

- Open the schema extension file in the extension folder.
- Locate the logical mapping for the field you want to remove in the upper `<documents>` section.
Use the `label` attribute to identify the proper field. For example, if the Available Field you want to remove is called **Contact**, search the `<attribute>` element that has the value `label="Contact"`.
- Add the following four attributes to the `<attribute>` element you want to remove from the Available Fields list:
 - `search="false"`
 - `list="false"`

```

    ■ detail="false"
    ■ create="false"
<documents name="rome">
  <document name="rKmDocument">
    <attribute name="contact" label="Contact" search="false"
    list="false" detail="false" create="false" />
  </document>
</documents>

```

Add search, list, detail,
and create attributes

These settings tell DocExplorer to hide the field on the search, list, detail, and create forms.

- 4 Save the schema extension file.

Changing the label a field displays in the Available Fields list

You can change the label that appears in the Available Fields list of personalized forms. Typically, you only need to add labels to new fields that you have added to a schema.

To change the label a field displays in the Available Fields list:

- 1 Open the schema extension file in the extension folder.
- 2 Locate the logical mapping for the field you want to change in the upper `<documents>` section.

Use the label attribute to identify the proper field. For example, if the Available Field you want to change is called **Contact**, search the `<attribute>` element that has the value `label="Contact"`.

- 3 Change the label attribute to the new desired value.

```

Update the label
attribute ————— <documents name="rome">
  <document name="rKmDocument">
    <attribute name="contact" type="string" label="Representative"/>
  </document>
</documents>

```

- 4 Save the schema extension file.

Changing the list of forms where a field is available or visible

You can determine the list of forms in which a field is available or visible. By default, a new field is available in all forms, but not visible. You can use personalization to make an available field visible on a form.

To change the list of forms where a field is available or visible:

- 1 Open the schema extension file in the extension folder.
- 2 Locate the logical mapping in the upper <documents> section for the fields whose availability you want to change.

Use the label attribute to identify the proper field. For example, if the Available Field you want to remove is called **Contact**, search the <attribute> element that has the value label="Contact".

- 3 Add one of the following values to make a field available or visible.

Location in Get-Answers menu	To make this form	Available	Visible	Neither available or visible
Reports	search	<ul style="list-style-type: none"> ■ search= ■ search =true 	search=true	search=false
Reports	list	<ul style="list-style-type: none"> ■ list= ■ list=true 	list=true	list=false
Workflows and Reports	detail	<ul style="list-style-type: none"> ■ detail= ■ detail=true 	detail=true	detail=false
Contribute New Document	create	<ul style="list-style-type: none"> ■ create= ■ create=true 	create=true	create=false

For example, the following settings make the contact field both available and visible in all forms:

```

<documents name="rome">
  <document name="rKmDocument">
    <attribute name="contact" type="string" label="Contact"
      search="true" list="true" detail="true" create="true" />
  </document>
</documents>

```

Set search, list, detail, and create attributes

- 4 Save the schema extension file.

Changing the physical mapping of a field

You can change the physical mapping that a field uses to point to another back-end database, table, or physical field.

To change the physical mapping of a field:

- 1 Open the rKmDocument.xml schema extension file in the extension folder.
- 2 In the lower <documents> section, change the physical mapping <attribute> element to match the new physical mapping you want.

The physical mapping <attribute> elements are between the <document> tags:

Change physical
mappings here

```
<documents name="rome">
  <document name="rKmDocument">
    <attribute field="_null" member="Product" name="Product"/>
    <attribute field="_null" member="Solution" name="Solution"/>
  </document>
</documents>
```

- a Change the field attribute to the new physical mapping.
- b Add any optional attributes you want to use for the physical mapping.

Refer to [<attribute>](#) on page 140 for more information on optional attributes of the <attribute> element.

- 3 Save the schema extension file.

Schema Elements and Attributes

All schemas use a standard set of XML elements and attributes that the Archway Document Manager recognizes. The following sections describe the XML elements and associated attributes that you can use to create valid schemas.

<?xml>

The <?xml> element is the standard XML namespace identifier. This element should always include the version attribute. All schemas require that this be the first element listed.

<schema>

The <schema> element is a required element of all schemas. The <schema> element functions as a container for the logical and physical mappings. The <schema> element does not have any attributes.

<documents>

Two sets of <documents> elements are required for each schema. One set of <documents> elements is the container for the logical mappings and the other set of <documents> elements is the container for the physical mappings.

Use in logical mapping

All schemas require one <documents> element where the name attribute has the value name="base". When this element has this name value, it becomes the container for the logical mappings.

Required attributes

- name. This attribute identifies the <documents> element container used by the logical mappings. This attribute must have the value name="base".

Optional attributes

- *None*. There are no optional attributes for the logical mapping portion of the schema.

Logical mappings always use name="rome"

```
<?xml version="1.0"?>
<schema>
  <documents name="rome">
    ...
  </documents>
  ...

```

Use in physical mapping

All schemas require at least one `<documents>` element where the name attribute has the value of an adapter name such as `name="rome"`. You can add one `<documents>` element for each adapter you want to provide physical mappings for. You can also support multiple versions of the same adapter if you use the version attribute.

Required attributes

- `name`. This attribute determines what adapter the schema uses to make connections to the back-end database. The value of this attribute must be an adapter name such as `name="rome"`.

<document>

You must add at least two sets of `<document>` elements to create a valid schema – one set for the logical mappings and another set for the physical mappings. You can add additional `<document>` elements in the physical mapping section if you want to support multiple adapters or multiple versions of the same back-end database.

Use in logical mapping

The logical mapping section uses the `<document>` elements as a container for the XML document that the Archway Document Manager produces. All XML elements produced by this schema will be child elements of the `<document>` element.

Required attributes

- `name`. This attribute determines what XML element the Archway Document Manager generates as the top-level element in any generated document using this schema. The value of this attribute must match the file name of the schema (*without* the `.xml` extension).

Optional attributes

- **ACLcreate**. This attribute determines the default access control list for DocExplorer forms that use this schema. The value of this attribute must be a capability word. Users who meet or exceed the capability word listed in this attribute will see a **New** button in DocExplorer forms that use this schema.
- **ACLdelete**. This attribute determines the default access control list for DocExplorer forms that use this schema. The value of this attribute must be a capability word. Users who meet or exceed the capability word listed in this attribute will see a **Delete** button in DocExplorer forms that use this schema.
- **ACLupdate**. This attribute determines the default access control list for DocExplorer forms that use this schema. The value of this attribute must be a capability word. Users who meet or exceed the capability word listed in this attribute will be able to edit fields in DocExplorer detail forms that use this schema.
- **create**. This attribute determines if a subdocument using this element is visible in DocExplorer *create* forms. The value of this attribute must be either true or false. Set the value to `create="true"` if you want this subdocument to be available on DocExplorer create forms. Set the value to `create="false"` if you want to prevent this subdocument from being available on DocExplorer create forms.
- **detail**. This attribute determines if a subdocument using this element is visible in DocExplorer *detail* forms. The value of this attribute must be either true or false. Set the value to `detail="true"` if you want this subdocument to be available on DocExplorer detail forms. Set the value to `detail="false"` if you want to prevent this subdocument from being available on DocExplorer detail forms.
- **docname**. This attribute defines the external schema that you want the Archway Document Manager to use to create a subdocument. The value of this attribute must match the file name of the schema (*without* the .xml extension) that you want to use for the subdocument. You only need this attribute if you want to create a subdocument using another schema.
- **label**. This attribute determines what name the schema has in DocExplorer forms that use this schema. The value of this attribute can be any text string. Typically, you will want to set this value to a user-friendly name describing the content of the schema.

- **list.** This attribute determines if a subdocument using this element is visible in DocExplorer *list* forms. The value of this attribute must be either true or false. Set the value to `list="true"` if you want this subdocument to be available on DocExplorer list forms. Set the value to `search="false"` if you want to prevent this subdocument from being available on DocExplorer list forms.
- **loadscript.** This attribute determines what ECMAScript function runs when this schema is used in a DocExplorer form. The value of this attribute must be the Peregrine Studio name of the ECMAScript function you want to run. You can use this script to load additional data for use by DocExplorer forms. This script uses the same XML message input as the form onload script.
- **preexplorer.** This attribute determines what ECMAScript runs when this schema is used in a DocExplorer form. The value of this attribute must be the Peregrine Studio name of the ECMAScript you want to run. You can use this script to make formatting changes to the XML message rendered by DocExplorer forms.
- **search.** This attribute determines if a subdocument using this element is visible in DocExplorer *search* forms. The value of this attribute must be either true or false. Set the value to `search="true"` if you want this subdocument to be available on DocExplorer search forms. Set the value to `search="false"` if you want to prevent this subdocument from being available on DocExplorer search forms.
- **subtypeprop.** This attribute determines whether this element inherits the attribute properties of the parent `<collection>` element. The value of this attribute must be `inherit` if you use the attribute at all. If you want this element to inherit the attribute properties set the value to `subtypeprop="inherit"`. If you want to specify the the attribute properties for this element, do not include a `subtypeprop` attribute.

Use in physical mapping

The physical mapping section uses the `<document>` elements to define the SQL name of the back-end database table.

Required attributes

- **name.** This attribute determines what XML element the Archway Document Manager matches to a back-end database table. The value of this attribute must match the file name of the schema (*without* the `.xml` extension). In Get-Answers, the name is `rome`.

Optional attributes

- **table.** This attribute identifies the table in the back-end database that the schema uses. The value of this attribute must be the SQL name of the table you want to use for source data. Each <document> element can only have one table attribute. To use data from other tables, you can create subdocuments within your schema. In Get-Answers, the table is rKmDocument.
- **preprocess.** This attribute determines what ECMAScript function runs *before* the Archway Document Manager connects to the back-end database. The value of this attribute must be the Peregrine Studio name of the ECMAScript function you want to run. You can use this script to format the request sent to the back-end database. For example, you can add additional SQL commands or validate that all required fields are listed in the request.
- **postprocess.** This attribute determines what ECMAScript runs *after* the Archway Document Manager receives a response from the back-end database. The value of this attribute must be the Peregrine Studio name of the ECMAScript you want to run. You can use this script to format the response sent from the back-end database. For example, you can sort the data by a particular criteria or return an error message if no records are found.

<attribute>

You must add at least two sets of <attribute> elements to create a valid schema – one set for the logical mappings and another set for the physical mappings.

Use in logical mapping

The logical mapping sections use the <attribute> elements to create an XML element in any document message built from this schema.

Required Attributes

- **name.** This attribute determines the XML tag that the Archway Document Manager generates when it uses the schema. The value of this attribute can be any string value. For example, if you set the value to name="contact" then the Archway Document Manager creates a <contact> XML tag. You must define at least one <attribute> element where the name attribute has the value name="id". This <attribute> element is required to uniquely identify each record returned by a schema query.
- **type.** This attribute determines what data format the elements uses as well as how Get-Answers renders the data in the user interface. The value of this attribute must be one of the following strings:

- attachment—This element is a path and file name to an attachment. Get-Answers renders this element as a collection of attachment controls.
- boolean—This element is a true or false string. Get-Answers renders this element as a check box.
- date—This element is a date listing. Get-Answers renders this element as a date edit control that includes a popup calendar.
- datetime—This element is a combined date and time listing. Get-Answers renders this element as a time edit control.
- id—This element is a number that uniquely describes a back-end database record. Get-Answers renders this element as a single-line edit field.
- image—This element is an image. Get-Answers renders this element as an imagefield.
- link—This element is a subdocument described elsewhere in the schema. Get-Answers renders this element a lookup field.
- memo—This element is a text string. Get-Answers renders this element a multi-line edit box.
- money—This element is a currency amount. Get-Answers renders this element a money field that includes a currency selection tool.
- number—This element is an integer. Get-Answers renders this element an editfield with spinner buttons.
- preload—This element is an executable script. Get-Answers runs the script listed in this element.
- string—This element is text. Get-Answers renders this element an editfield.
- time—This element is a time listing. Get-Answers renders this element as a time edit control.
- url—This element is a Web site address. Get-Answers renders this element as an HREF link icon.

Note: The Archway Document Manager does not validate that the contents of an element matches the type attributed listed for it.

Optional attributes

- access. This attribute determines if the element is read-only or editable in DocExplorer forms. The value of this attribute must be either r or null. Set the value to access="r" if you want to make this element read-only. Clear the value or remove the attribute if you want to make the element editable.

- **ACLcreate.** This attribute determines the default access control list for DocExplorer forms that use this element. The value of this attribute must be a capability word. Users who meet or exceed the capability word listed in this attribute will see this element in DocExplorer *create* forms that use this schema.
- **ACLdetail.** This attribute determines the default access control list for DocExplorer forms that use this element. The value of this attribute must be a capability word. Users who meet or exceed the capability word listed in this attribute will see this element in DocExplorer *detail* forms that use this schema.
- **ACLlist.** This attribute determines the default access control list for DocExplorer forms that use this element. The value of this attribute must be a capability word. Users who meet or exceed the capability word listed in this attribute will see this element in DocExplorer *list* forms that use this schema.
- **ACLsearch.** This attribute determines the default access control list for DocExplorer forms that use this element. The value of this attribute must be a capability word. Users who meet or exceed the capability word listed in this attribute will see this element in DocExplorer *search* forms that use this schema.
- **create.** This attribute determines if the element is visible in DocExplorer *create* forms. The value of this attribute must be either true or false. Set the value to `create="true"` if you want this field to be available on DocExplorer create forms. Set the value to `create="false"` if you want to prevent this field from being available on DocExplorer create forms.
- **detail.** This attribute determines if the element is visible in DocExplorer *detail* forms. The value of this attribute must be either true or false. Set the value to `detail="true"` if you want this field to be available on DocExplorer detail forms. Set the value to `detail="false"` if you want to prevent this field from being available on DocExplorer detail forms.
- **label.** This attribute determines what name the element has in DocExplorer Available Field list. The value of this attribute can be any text string. Typically, you will want to set this value to a user-friendly name describing the content of the field.
- **list.** This attribute determines if the element is visible in DocExplorer list forms. The value of this attribute must be either true or false. Set the value to `list="true"` if you want this field to be available on DocExplorer list forms. Set the value to `list="false"` if you want to prevent this field from being available on DocExplorer list forms.

- **required.** This attribute determines if this element requires a value in order to insert or update a record in the back-end database. The value of this attribute must be either true or false. Set the value to `required="true"` if you want to make the element a required input field when it is added to DocExplorer forms.
- **search.** This attribute determines if the element is visible in DocExplorer *search* forms. The value of this attribute must be either true or false. Set the value to `search="true"` if you want this field to be available on DocExplorer search forms. Set the value to `search="false"` if you want to prevent this field from being available on DocExplorer search forms.

Use in physical mapping

The physical mapping sections use the `<attribute>` elements to define the fields in the back-end database that map to each logical mapping.

Required Attributes

- **name.** This attribute determines the XML tag in which the Archway Document Manager places query results. The value of this attribute must match an element defined in the logical mapping section.
- **field.** This attribute identifies the field in the back-end database that you want the schema to use for document queries. The value of this attribute must be the SQL name of the field you want to use for the data source.
- **member.** The value of this attribute must be the SQL name of the field you want to use for the data source. `field` is used by the rome adapter and must have the same value as the `name` field.

Documents

The Archway Document Manager uses schemas to create documents, which are XML messages created from the following components:

- **Schema logical definitions.** The schema logical definitions determine what XML elements make up the generated document.
- **The return values of database queries.** The Archway Document Manager uses the schema physical mappings to create database queries. The return values of these queries determine the content of the elements and attributes of the generated document.
- **ECMAScript formatting.** ECMAScript functions can modify a document before and after any queries have been made to the back-end database.

The final output of these three processes is an XML document that the Archway Document Manager renders as HTML in the interface.

You can see the raw XML documents by enabling the **Show form information** option from the Administration settings. The form information window displays the following document information:

- **Script Input.** This tab displays the document submitted to the current form from the output of a previous form. For example, a list form displays the output of a prior search form. This document is passed to the form onload script as an input parameter.
- **Script Output.** This tab displays the document generated by the output of the current form's onload script. Typically, each onload script invokes a schema that queries the back-end database for relevant information. For example, a form will invoke a database query through the schema.
- **PreXSL.** This tab displays the document after the Archway servlet has processed the document and prepared it to be rendered by the client-side browser.

7 Get-Answers Administration

CHAPTER

This chapter includes instructions for administering your Get-Answers system.

Topics in this chapter include:

- *Accessing the Peregrine Portal Admin module* on page 146
- *Using the Control Panel* on page 148
- *Viewing the Deployed Versions* on page 149
- *Viewing the Server Log* on page 150
- *Using the Settings page* on page 150
- *Verifying Script Status* on page 153
- *Displaying Message Queues* on page 153
- *Showing Queue Status* on page 154
- *Importing and exporting personalizations* on page 155
- *Viewing adapter transactions* on page 155
- *Using the IBM Websphere Portal* on page 156
- *Displaying form information* on page 156
- *User self-registration* on page 159
- *Changing passwords* on page 160
- *Logging and monitoring user sessions* on page 160

Accessing the Peregrine Portal Admin module

The Peregrine Portal administrator login page enables access to the Peregrine Portal Admin module. You use the Admin module to define the settings for your Peregrine system.

Note: After installing and building Get-Answers, you must log in as a ServiceCenter user with `getit.admin` rights to access the Admin module and administer the Get-Answers integration with ServiceCenter. For a list of access capability words and Adapter configuration instructions, see the section on Get-Answers security in this guide.

A default administrator, System, gives you access to the Admin module without being connected to a back-end system. After you configure your user name on the Common tab, you can also access the Admin module from the Navigation menu.

Important: When you change parameters using the Admin module, a `local.xml` file is created in the `\<appsrvr>\WEB-INF` directory (where *appsrvr* is the path to your application server) to store these parameters. If you reinstall Get-Answers, make a copy of this file and store it outside your Get-Answers installation. Failure to do this will result in your parameter values being lost during the new installation.

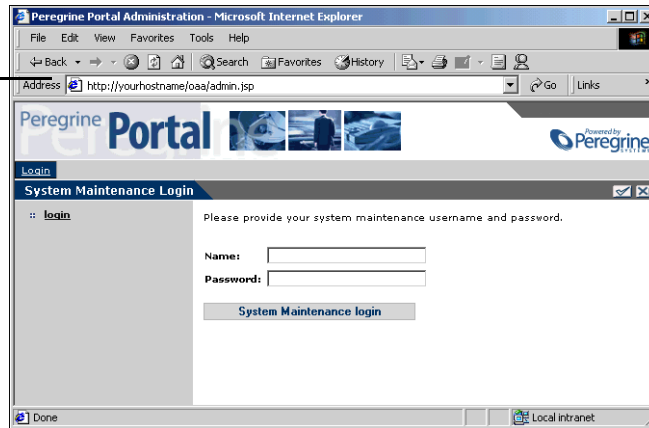
To access the Peregrine Portal administrator login page:

- 1 Verify that your application server (for example, Tomcat) is running.
- 2 In your Web browser Address field, type:
`<hostname>/oaa/admin.jsp`

3 Press Enter to open the Portal administrator login page.

Type your hostname to connect to your local server.

System is the default administrator name.



- 4 In the Name field, type **System**.
No password is required on initial login.
- 5 Click **System Maintenance login** to open the **Control Panel** page.

Administrators use the Admin module to define settings to the system.

Here is a list of the adapters currently registered in this server. If necessary, you may also reset the server and all its connections.

Target	Adapter	Status
weblocation	com.peregrine.ooa.adapter.scSCAdapter	connected
mail	com.peregrine.ooa.adapter.mail.MailAdapter	connected
portalDB	com.peregrine.ooa.adapter.scSCAdapter	connected
sc	com.peregrine.ooa.adapter.scSCAdapter	connected

Server Name	Last Min.	5 Min. Avg.	20 Min. Avg.	Peak
localhost	1	1	1	2

Server Name	Last Min.	5 Min. Avg.	20 Min. Avg.	Peak
localhost	0	0	0	15

[Reset Server](#)

The activities available in the Admin module include:

Select this option	To do the following
Control Panel	view the status of connections to the back-end systems.
Deployed Versions	view the list of deployed applications with version numbers on this server.
Server Log	view activity on the Get-Answers server.
Settings	view and change settings for the Peregrine Portal.
Show Script Status	view and verify which scripts are running. You can also start and stop scripts from this window.
Show Message Queues	view a list of all message queues.
Show Queue Status	view the current status of the queues: operational and unlocked, or suspended.
Import / Export	move Personalizations from a development to a production environment.
Adapter Transactions/Minute	view the transactions per minute for the back-end adapter.
IBM Websphere Portal Integration	view the installed OAA portal components in the IBM WPS environment

Using the Control Panel

Use the Control Panel page to check the status of the connections to the databases you are accessing with Get-Answers and your Web applications. You can also reset the connection between the Archway servlet and the adapters to the back-end systems.

To reset the connection between the Archway servlet and back-end system:

- ▶ Click **Reset Server**.

A message at the top of the page indicates that the connections are reset.

Informational, warning, and error messages appear at the top of the page.

The Archway servlet and its Adapter connections have been reset successfully.

Here is a list of the adapters currently registered in this server. If necessary, you may also reset the server and all its connections.

Target	Adapter	Status
webication	com.peregrine.aaa.adapter.sc.SCAAdapter	connected
mail	com.peregrine.aaa.adapter.mail.MailAdapter	connected
portalDB	com.peregrine.aaa.adapter.sc.SCAAdapter	connected
sc	com.peregrine.aaa.adapter.sc.SCAAdapter	connected

Server Name	Last Min.	5 Min. Avg.	20 Min. Avg.	Peak
localhost	1	1	1	2

Server Name	Last Min.	5 Min. Avg.	20 Min. Avg.	Peak
localhost	1	0	0	15

[Reset Server](#)

Viewing the Deployed Versions

The Deployed Versions screen lists all of the packages that deploy during the installation, including the version number of each package.

To view the Deployed Versions list:

- 1 From the Activity menu, select **Deployed Versions**.
A list of the installed packages opens.

Current applications and their versions are available for viewing with the Deployed Versions option.

This is the list of deployed applications with version numbers on this server.

Applications	Versions
Peregrine Enterprise Portal Accessibility Theme	accessibletheme.4.1.0.5
OAA Archway Servlet	archway.4.1.0.27
Peregrine Enterprise Portal Baja Theme	bajatheme.4.1.0.4
Peregrine Enterprise Portal Classic Theme	classitheme.4.1.0.4
OAA Core Application	core.4.1.0.23
Get-Services Change Request	get-services-change-request.4.1.0.16
Get-Services Change	get-services-change.4.1.0.15
Get-Services	get-services.4.1.0.10
Get-IT Common Utilities	getitcommon.4.1.0.10
Mail Adapter	mailadapter.4.1.0.4
Peregrine Enterprise Portal	portal.4.1.0.28
Peregrine Enterprise Portal Quicksilver Theme	quicksilvertheme.4.1.0.4
ServiceCenter Adapter	scadapter.4.1.0.7
Peregrine Enterprise Portal Sierra Theme	sierratheme.4.1.0.5

[Print](#)

- 2 Click **Print** for a printout of this list.

Viewing the Server Log

The Server Log provides a history of server events. The default file name is `archway.log`.

To view the Server Log:

- 1 From the Activity menu, select **Server Log**.

A form opens with a drop-down list for you to select the log you want to view.

You can view the log file from your Web browser or download it to your preferred location.



- 2 Click the drop-down and select the log file you want to view.
- 3 Set the number of lines to view.
- 4 Do one of the following:
 - Click **View** to see the log file from your Web browser.
 - Click **Download** to initiate the File Download wizard that downloads the `archway.log` file to a location of your choice.

Using the Settings page

On the Activity menu, click **Settings** to open the current parameter settings. The Settings page is divided into tabs. The tabs that you see depend on the Web applications that you installed and the adapters that you use. The Common tab is available for all installations.

Settings for the Portal, PortalDB, and Web Application tabs are set during the installation (refer to the *Get-Answers Installation Guide*). You can access the Settings page at any time to change the installation settings. Set the E-mail tab only when users have access to self-registration (see *User self-registration* on page 159).

To view Settings:

- From the Activity menu, click **Settings**.

Each parameter on the tab has a description that guides you through the settings.

The tabs you see on the Settings page depend on the Web applications you installed.

The screenshot shows the 'Admin Settings' window with several tabs: Common, E-mail, Get-Answers, Get-Answers Portal, Logging, NotificationDB, Notification Services, Portal, Portal DB, rome, and Themes. The 'Common' tab is active, displaying the following settings:

- Maximum attached file size (in KB):** 0. Description: The size limit, in KB, of files that may be submitted as attachments. A value of 0 indicates that no limit is set. This setting is a default that can be overridden by individual attachment fields.
- Common Backend:** rome. Description: Adapter target name used to support common user operations. [Click for default: \[portalDB\]](#)
- List of target aliases:** weblication;mail. Description: Specifies a list of semicolon delimited target aliases used by web applications in this package.
- System Maintenance username:** System. Description: The system maintenance username. This login provides access to administrative functionality. The system maintenance user is independent of any deployed adapter(s). Use this login to configure a newly installed system or to troubleshoot an existing install.
- System Maintenance password:** [Empty]. Description: The system maintenance password.
- Application path:** WEB-INF/apps/. Description: Directory location of the Peregrine Portal Web Applications.
- Event queue:** rome. Description: Enter the name of the adapter that should be used by the Peregrine Portal event queue engine. For example:
 - To use ServiceCenter's repository, enter "sc"
 - To use AssetCenter's repository, enter "ac"[Click for default: \[portalDB\]](#)

The 'Language Translation' section is also visible, with the following settings:

- Translation Server Factory Class:** com.peregrine.util.WTSLanguageTranslatorFactory. Description: The Java factory class which generates the proper class associated with the Translation Server.
- Language from which to translate:** English. Description: The language from which to translate or the base language in which all text is currently displayed as.
- Translation Server IP Address:** [Empty]. Description: The IP address of the Translation Server. This address may or may not contain a

Setting parameters using the Admin module

When you make changes using the Admin Settings page, a `local.xml` file is created in the `C:\<appsvr>\WEB-INF` directory. All changes to property settings are stored in this file. Restart Tomcat after making changes that are stored in `local.xml`.

Important: If you change parameters on the Admin Settings page and then need to reinstall Get-Answers, it is important that you copy the `local.xml` file to a location other than your Get-Answers installation, or all of your settings will be lost when you redeploy Get-Answers. After the installation, move the copy back to the `WEB-INF` directory.

To define a parameter:

- 1 Locate the setting you want to change and type the new parameter.
Note: If you have previously changed a setting and want to return to the default setting, click the **Click for default** link displayed in the description area for the parameter you want to revert. This link appears only when a setting is different from the default.
- 2 Scroll to the bottom of the page, and then click **Save**.
Note: You must click **Save** on each page before making changes to another setting.

The Control Panel opens.

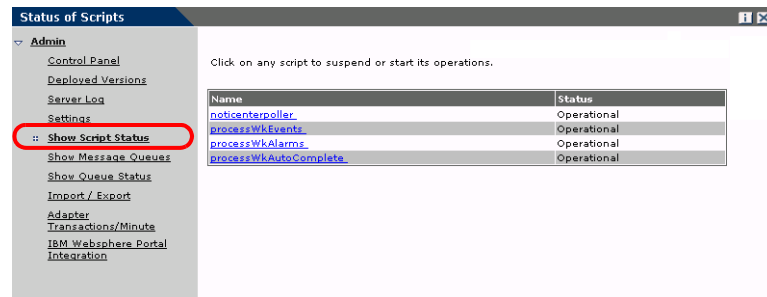
- 3 Click **Reset Server**.
An information message at the top of the Control Panel indicates that the server has been reset.

Verifying Script Status

The Script Status page lists the name and status of any script that is currently running.

To verify the script status:

- 1 From the Administration Activity menu, click Show Script Status to display the Status of Scripts page that shows the name of each script.



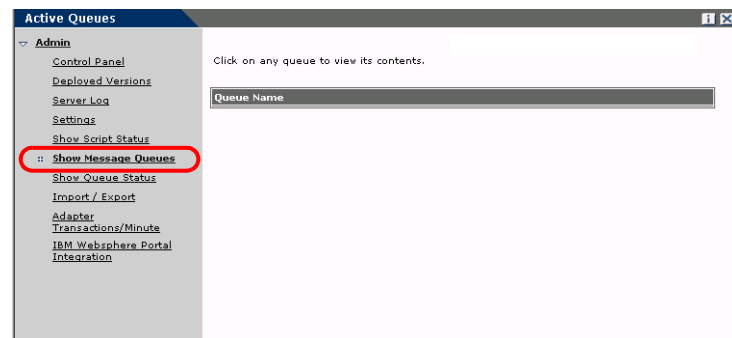
- 2 Click on the script to suspend it.

Displaying Message Queues

The Message Queues are displayed whenever a queue has data waiting to be transferred.

To display message queues:

- 1 From the Administration Activity menu, click Show Message Queues to display the Active Queues page.



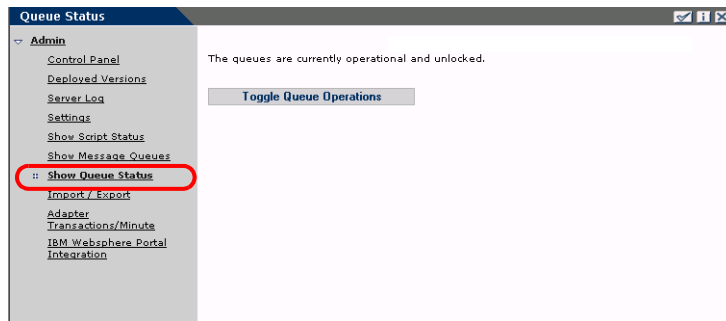
- 2 Click the queue name in the list to view the contents of a queue.

Showing Queue Status

Use the Show Queue Status option to verify or change the status of the message queues.

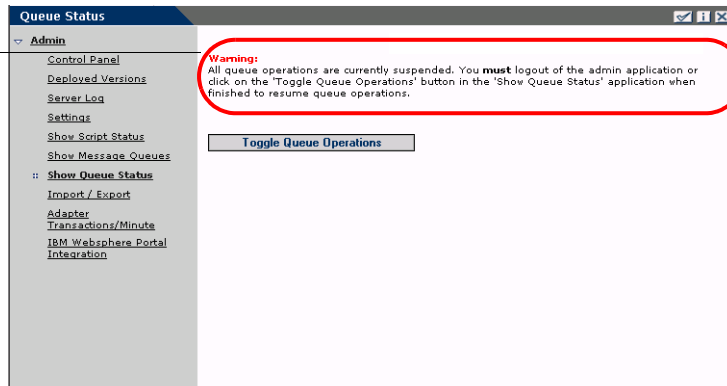
To show queue status:

- 1 From the Activity menu, click **Show Queue Status** to open the Queue Status page.



- 2 Click **Toggle Queue Operations** to change the status to suspended.

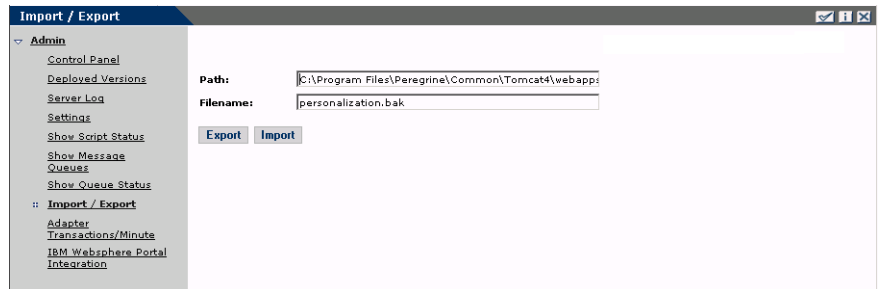
A warning message indicates that the Queue Status is suspended.



- 3 Click **Toggle Queue Operations** to return to the operational status.

Importing and exporting personalizations

You can move personalizations that you created in a development environment to a production environment. See *Using the Personalization Interface* chapter in this guide for detailed instructions on importing and exporting the personalizations. Select the **Import/Export** option from the Admin activity menu to access the page.

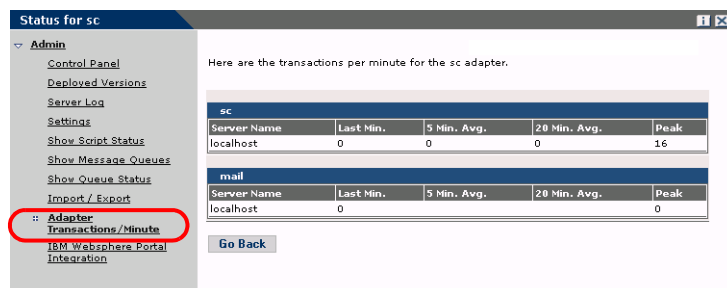


Viewing adapter transactions

You can track your adapter transactions by viewing the adapter Status page.

To view adapter transactions per minute:

- From the Activity menu, click **Adapter Transactions/Minute** to open the adapter Status page.



Using the IBM Websphere Portal

You can generate an IBM Websphere Portal Server web archive (war) file configured with references to installed OAA portal components.

To generate a war file:

- 1 From the Activity menu, click **IBM Websphere Portal Integration** to open the **Portal Integration** page.

- 2 Enter the following information:
 - source path
 - destination path
 - base URL
- 3 Click **Generate WAR File**.

Displaying form information

You can use the Admin module to configure Web application forms to display the location and file name of the current form.

To display form information:

- 1 From the Admin module, click **Settings**, then **Logging**.

2 Scroll to the Show form info field, and click Yes if necessary.

Set Show Form Info to Yes.

The screenshot shows the 'Admin Settings' window with the 'Logging' tab selected. The 'Show form info' checkbox is checked and circled in red. A red arrow points from the text 'Set Show Form Info to Yes.' to this checkbox. The 'Log domains' list is empty, and the 'Debug script' checkbox is also selected.

3 Click Save.

The Control Panel opens.

4 Click Reset Server.

The name of the form is at the top of each form.

The form name is at the top of the page.

Click the Display Form Info button to view the form composition.

The screenshot shows the 'Admin Settings' window with the 'Common' tab selected. The 'Project.common.admin.settings.start' button is circled in red. A red arrow points from the text 'Click the Display Form Info button to view the form composition.' to this button. The 'Maximum attached file size' is set to 0, and the 'Common Backend' is set to portalDB.

Displaying form details

You can also display detailed information about the current form. Click the **Display Form Info** button at the top right of the form. A separate window opens.

View the contents in each tab for more information about the form.

```
<?xml version="1.0" encoding="UTF-8"?>
<_doc>
  <_docExplorerView/>
  <_docExplorerModel>
    <target>portalDB</target>
    <_docExplorerContext>AdminSettings</_docExplorerContext>
    <_docExplorerInstance/>
    <_DocExplorerBackend>weblication</_DocExplorerBackend>
    <_docExplorersSubType/>
    <_docExplorerAction>detail</_docExplorerAction>
    <_form>e_admin_settings_start.do</_form>
    <_module>common</_module>
    <_module>admin</_module>
    <_activity>settings</_activity>
    <_formname>start</_formname>
    <_return/>
    <_count>20</_count>
    <_tabs>
      <tab balloon="$$$ID$(common,configPortalLabel)" caption="$$$ID$(common,configPortalLabel)" url="e_admin_settings_start.do?target=portal"/>
      <tab balloon="$$$ID$(common,configCommonLabel)" caption="$$$ID$(common,configCommonLabel)" url="e_admin_settings_start.do?target=common"/>
      <tab balloon="$$$ID$(incidentmgt,configProblemTabLabel)" caption="$$$ID$(incidentmgt,configProblemTabLabel)" url="e_admin_settings_start.do?target=incidentmgt"/>
      <tab balloon="$$$ID$(common,configPortalDBLabel)" caption="$$$ID$(common,configPortalDBLabel)" selected="true" url="e_admin_settings_start.do?target=portalDB"/>
      <tab balloon="$$$ID$(common,configThemesLabel)" caption="$$$ID$(common,configThemesLabel)" url="e_admin_settings_start.do?target=themes"/>
      <tab balloon="$$$ID$(common,configWeblicationLabel)" caption="$$$ID$(common,configWeblicationLabel)" url="e_admin_settings_start.do?target=weblication"/>
      <tab balloon="$$$ID$(common,configLoggingLabel)" caption="$$$ID$(common,configLoggingLabel)" url="e_admin_settings_start.do?target=logging"/>
      <tab balloon="$$$ID$(common,configScLabel)" caption="$$$ID$(common,configScLabel)" url="e_admin_settings_start.do?target=sc"/>
      <tab balloon="$$$ID$(mailadapter,Label)" caption="$$$ID$(mailadapter,Label)" url="e_admin_settings_start.do?target=mail"/>
      <tab balloon="$$$ID$(changerequestmgt,configChangeTabLabel)" caption="$$$ID$(changerequestmgt,configChangeTabLabel)" url="e_admin_settings_start.do?target=changemgt"/>
    </_tabs>
    <_locale>en</_locale>
  </_docExplorerModel>
</_doc>
```

The form has the following tabs:

This tab	Contains
Script Input	the script that sends a request to the back-end system.
Script Output	the information returned by the script request to the back-end system.
User Session	details about the current user session, including browser type, back-end system version, and the access rights established for this user.
Log	a list of actions taken by the script to execute the form.
PreXSL	output from XSL before it gets rendered to the browser.
Browser Source	HTML source code for the current page.
BackChannel Source	HTML source code for frames where the data is stored.
Application Channel Source	HTML source code for the shared applications.

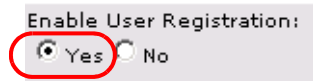
This tab	Contains
Tab Source	HTML source code for tabs.
Menu Source	HTML source code for menus.
Sync/Update Window	HTML source code to synchronize with the page and reload.
Help	Help for debugging the window.

User self-registration

With the Admin module, administrators can choose to have end users self-register for new accounts from the login screen if the user is not already in the ServiceCenter database. When the user registers, ServiceCenter creates an Operator record and a Contact record for the new user with basic user login rights. See the chapter on *Security* in this guide for more information on the registration process.

To enable users to self-register from the Login screen:

- 1 From the Admin module Settings page, click **Common**.
- 2 Scroll to **Enable User Registration**.



Click Yes to give users the ability to self-register for new accounts.

- 3 Click **Yes**.

Tip: When using an application with ServiceCenter 5.0 as the back-end system, the first name and last name are reversed in the ServiceCenter contact record from the format used in an OAA Platform application.

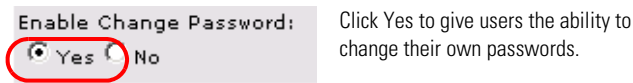
ServiceCenter 5.0 stores names in the format last name/first name. The OAA Platform stores names in the format first name/last name. As a temporary solution, you can change the way operator names are handled in ServiceCenter using the **Use Operator Full Name?** option in the Environment records for Incident and Service Managements. Refer to the *ServiceCenter 5.0 Application Administration Guide* for instructions.

Changing passwords

Using the Admin module, administrators can choose to have end users change their own passwords from the Home page.

To enable users to change passwords:

- 1 From the Admin module Settings page, click **Common**.
- 2 Scroll to **Enable Change Password**.



- 3 Click Yes.

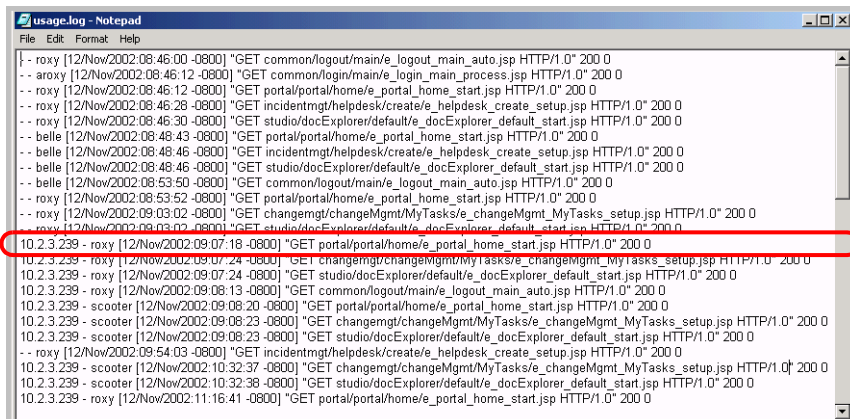
Logging and monitoring user sessions

The `usage.log` file has a record of user logins that is in the `bin` directory of your application server installation. With this file, you can determine which application is in use and how many users access an application during a day.

Understanding the `usage.log` file

The following line shows an excerpt from a `usage.log` file:

```
10.2.3.239 - roxy [12/Nov/2002:09:07:18 -0800] "GET
portal/portal/home/e_portal_home_start.jsp HTTP/1.0" 200 0
```



```
usage.log - Notepad
File Edit Format Help
[12/Nov/2002:08:46:00 -0800] "GET common/logout/main/e_logout_main_auto.jsp HTTP/1.0" 200 0
-- aroxy [12/Nov/2002:08:46:12 -0800] "GET common/login/main/e_login_main_process.jsp HTTP/1.0" 200 0
-- roxy [12/Nov/2002:08:46:12 -0800] "GET portal/portal/home/e_portal_home_start.jsp HTTP/1.0" 200 0
-- roxy [12/Nov/2002:08:46:28 -0800] "GET incidentmgmt/helpdesk/create/e_helpdesk_create_setup.jsp HTTP/1.0" 200 0
-- roxy [12/Nov/2002:08:46:30 -0800] "GET studio/docExplorer/default/e_docExplorer_default_start.jsp HTTP/1.0" 200 0
-- belle [12/Nov/2002:08:48:43 -0800] "GET portal/portal/home/e_portal_home_start.jsp HTTP/1.0" 200 0
-- belle [12/Nov/2002:08:48:46 -0800] "GET incidentmgmt/helpdesk/create/e_helpdesk_create_setup.jsp HTTP/1.0" 200 0
-- belle [12/Nov/2002:08:48:46 -0800] "GET studio/docExplorer/default/e_docExplorer_default_start.jsp HTTP/1.0" 200 0
-- belle [12/Nov/2002:08:53:50 -0800] "GET common/logout/main/e_logout_main_auto.jsp HTTP/1.0" 200 0
-- roxy [12/Nov/2002:08:53:52 -0800] "GET portal/portal/home/e_portal_home_start.jsp HTTP/1.0" 200 0
-- roxy [12/Nov/2002:09:03:02 -0800] "GET changemgmt/changeMgmt/MyTasks/e_changeMgmt_MyTasks_setup.jsp HTTP/1.0" 200 0
-- roxy [12/Nov/2002:09:03:02 -0800] "GET studio/docExplorer/default/e_docExplorer_default_start.jsp HTTP/1.0" 200 0
10.2.3.239 - roxy [12/Nov/2002:09:07:18 -0800] "GET portal/portal/home/e_portal_home_start.jsp HTTP/1.0" 200 0
10.2.3.239 - roxy [12/Nov/2002:09:07:24 -0800] "GET changemgmt/changeMgmt/MyTasks/e_changeMgmt_MyTasks_setup.jsp HTTP/1.0" 200 0
10.2.3.239 - roxy [12/Nov/2002:09:07:24 -0800] "GET studio/docExplorer/default/e_docExplorer_default_start.jsp HTTP/1.0" 200 0
10.2.3.239 - roxy [12/Nov/2002:09:08:13 -0800] "GET common/logout/main/e_logout_main_auto.jsp HTTP/1.0" 200 0
10.2.3.239 - scooter [12/Nov/2002:09:08:20 -0800] "GET portal/portal/home/e_portal_home_start.jsp HTTP/1.0" 200 0
10.2.3.239 - scooter [12/Nov/2002:09:08:23 -0800] "GET changemgmt/changeMgmt/MyTasks/e_changeMgmt_MyTasks_setup.jsp HTTP/1.0" 200 0
10.2.3.239 - scooter [12/Nov/2002:09:08:23 -0800] "GET studio/docExplorer/default/e_docExplorer_default_start.jsp HTTP/1.0" 200 0
-- roxy [12/Nov/2002:09:54:03 -0800] "GET incidentmgmt/helpdesk/create/e_helpdesk_create_setup.jsp HTTP/1.0" 200 0
10.2.3.239 - scooter [12/Nov/2002:10:32:37 -0800] "GET changemgmt/changeMgmt/MyTasks/e_changeMgmt_MyTasks_setup.jsp HTTP/1.0" 200 0
10.2.3.239 - scooter [12/Nov/2002:10:32:38 -0800] "GET studio/docExplorer/default/e_docExplorer_default_start.jsp HTTP/1.0" 200 0
10.2.3.239 - roxy [12/Nov/2002:11:16:41 -0800] "GET portal/portal/home/e_portal_home_start.jsp HTTP/1.0" 200 0
```


Each login is on a line. Within one user session, each module logs only one line.

The following table shows the meaning of each element in the log entry:

Remote Host	Rfc931	User Login	Date	Request	Status	Bytes
10.2.3.239	-	roxy	[12/Nov/2002:09:07:18 -0800]	"GET portal/portal/home/e_portal_home_start.jsp HTTP/1.0"	200	0

This element	Contains
Remote Host	the remote host name or IP address if the DNS host name is not available or was not provided.
Rfc931	the remote login name of the user. This is always a dash because this information is not needed.
User Login	the user name authenticated to log in to the Peregrine Portal.
Date	the date and time of the request.
Request	the module accessed by the user. The name of the module is the first part of the GET parameter. In the previous above, the module accessed is <i>notificationsservices</i> , the location of the login script.
Status	the HTTP response code returned to the client. This value is always 200 to specify that it was a valid request.
Bytes	the number of bytes transferred. The number is always entered as 0, because this information is not needed.

8 Get-Answers Security

CHAPTER

This chapter describes the different security configuration options available in Get-Answers. Topics in this chapter include:

- *Password encoding methods* on page 164
- *User registration* on page 165
- *Authenticating users* on page 166
- *Default security configuration* on page 167
- *Custom JAAS configuration* on page 168
- *Standard Sun Microsystems JAAS configuration* on page 177
- *Integrated Windows Authentication* on page 178
- *Integrating with single sign-on tools* on page 187
- *Contact-based authentication* on page 190
- *Creating an alternate login page* on page 195

Password encoding methods

By default, Get-Answers does not encode passwords sent over the network. Get-Answers sends plain text passwords to the authenticating back-end databases and stores plain text passwords in a browser cookie if the user selects to **enable automatic login**. If you want to secure your Get-Answers passwords, you have three options:

- Enable Secure Sockets Layer (SSL) on your Web server
- Configure Get-Answers to use a directory service such as LDAP
- Enable your Web server to use Windows NT Challenge/Response

In order to use SSL, you need to acquire a digital certificate. If your Web server has a certificate, then your Get-Answers login URL must include the **https** protocol indicator. After the user browser has made a secure connection to the Web server, all data transferred is encrypted. Refer to your Web server documentation for information on configuring SSL.

Get-Answers also supports authentication via a directory service such as LDAP. When you authenticate to a directory service, Get-Answers passes SHA hash encoding passwords to the service. For instructions configuring a directory service see *Custom JAAS configuration* on page 168.

Get-Answers also supports Integrated Windows Authentication. When this form of authentication is used, passwords are not actually exchanged between the browser and Web server, and the authentication process is kept secure. However, Integrated Windows Authentication is only supported by Internet Explorer browsers on Windows systems. For instructions configuring Integrated Windows Authentication see *Integrated Windows Authentication* on page 178.

User registration

All Get-Answers users need a login account. If a user is attempting to log in for the first time, the user is prompted for certain default information as shown in the following page. The first four fields are required, as indicated by the arrows to the right of each field.

The screenshot shows the 'User Information' registration page. It features a navigation bar with 'Login' and 'User Information' tabs. The 'User Information' tab is active, showing a 'Register' link and a registration form. The form contains five input fields: 'First Name', 'Last Name', 'Login Name', 'Email Address', and 'Phone Number'. The first four fields have small blue arrows to their right, indicating they are required. A 'Register' button is located below the form. The page also includes a 'Powered by Peregrine' logo in the top right and a 'Local intranet' link in the bottom right.

When the user clicks **Register**, the information is stored in the appropriate database.

Basic registration information and login scripts are stored in the `.../oaa/apps/common/jscript/` directory. Login scripts are in the `login.js` file. If you want to make changes to the registration process, such as changing the way a user's password is defined, you can change the scripts in this directory.

Enabling the E-mail adapter

If users have the ability to self-register, you must make sure that the E-mail tab from the Get-Answers Admin module Settings page contains the MailAdapter name.

The MailAdapter is an implementation of JavaMail API 1.2 and supports the following mail protocols:

- POP3 for inbound mail

- IMAP for inbound mail
- SMTP for outbound mail

The MailAdapter also supports MIME type attachments in outbound e-mail.

Set the following parameters, as needed, on the E-mail tab of the Admin module Settings page.

Portal	Common	Portal DB	Web Application	Logging	XSL	E-mail
Inbound mail host: The full name or IP address of the machine hosting the inbound mail server. If this field is empty, then the status of the mail adapter will indicate the status of the outbound mail server connection.						
mailhost						
Inbound mail protocol: The protocol used by the inbound mail server, which is either imap or pop3.						
imap						
Inbound mail user ID: The user ID used to access the inbound mail server.						
Inbound mail password: The user password used to access the inbound mail server.						
Mail sender address: This address is used as the default sender address in outbound email messages.						
Legal domains: Enter a semicolon-separated list of mail domains that the Peregrine Portal may correspond with. Only users with an email address in these domains are allowed to complete online self-registration.						
perigrine.com;apxydev.com;getmarketaccess.com						
Anonymous user: Anonymous user name used when an unknown user attempts to communicate with the mail adapter						
falcon						
Anonymous password: Anonymous user password for the mail adapter						
Outbound mail host: The full name or IP address of the machine hosting the outbound mail server. Click for default: mailhost 						
condor.peregrine.com						
Outbound mail user ID: The user ID used to access the outbound mail server.						
Outbound mail password: The user password used to access the outbound mail server.						
Adapter: Full class path for adapter associated with this target.						
com.peregrine.oaa.adapter.mail.MailAdapter						
<input type="button" value="Save"/>						

Type the name of your MailAdapter in the Adapter field.

Troubleshooting the MailAdapter connection

You can check the status of the MailAdapter connection on the Control Panel. If the adapter shows as *disconnected*, check that the settings on the E-mail tab of the Settings page are correct. If you are still unable to connect, contact your system administrator for verification of the parameter values.

Authenticating users

You can configure the Peregrine OAA Platform to use one of five security authentication options:

- Use the default configuration to authenticate users against Peregrine adapters. See *Default security configuration* on page 167.

- Use a custom configuration to authenticate users against user-defined adapters such as LDAP or JDBC compliant databases. See *Custom JAAS configuration* on page 168.
- Use a standard JAAS configuration to authenticate users against the Sun Microsystem's standard Java Authentication and Authorization Service (JAAS). See *Standard Sun Microsystems JAAS configuration* on page 177.
- Use Integrated Windows authentication to authenticate users and pass the information to the Web application. See *Integrated Windows Authentication* on page 178.
- Use an alternate login page and authenticate users against any of the other login options. See *Creating an alternate login page* on page 195.

Once a user is authenticated, the modules to which the user has access are defined by the back-end system. If you are using ServiceCenter for the back-end system, the user must have the appropriate capability words set in the Operator record in ServiceCenter in order to see the corresponding module in the web application.

Default security configuration

The default configuration authenticates users against a set of pre-configured JAAS login modules. By default, one JAAS login module is configured for each registered Peregrine adapter. For example, if you are using both AssetCenter and ServiceCenter, then Get-Answers creates login modules for *both* the ACAdapter and the SCAdapter.

These login modules are *only* used to authenticate users. User access rights are derived from user profile records in the back-end systems (for example, ServiceCenter or AssetCenter). User access rights determine which modules the user can access and what tasks they can perform within those modules. For example, one user can open tickets only, while another has rights to approve tickets as well.

You do not have to do any additional configuration to use the default security configuration. Get-Answers automatically generates login modules for each Peregrine adapter installed on the system.

The default login module settings are:

- loginModule=com.peregrine.OAA.security.OAALoginModule

- control flag=OPTIONAL
- options=<none>

Custom JAAS configuration

A custom JAAS configuration authenticates users against a set of JAAS LoginModules you define in a `local.xml` file. This file contains the settings to use for each JAAS LoginModule. A `<jaas_config>` entry in `local.xml` has the following format.

```
<jaas_config>

  <jaasConfiguration>CustomConfig</jaasConfiguration>
  <CustomConfig>adapter1;adapter2</CustomConfig>

  <adapter1>
    <loginModule>Java class of login module</loginModule>
    <controlFlag>authentication behavior</controlFlag>
    <options>semicolon separated list of options</options>
  </adapter1>

  <adapter2>
    <loginModule>Java class of login module</loginModule>
    <controlFlag>authentication behavior</controlFlag>
    <options>semicolon separated list of options</options>
  </adapter2>

</jaas_config>
```

The following table describes how to use the XML tags and assign appropriate values.

Important: XML is case sensitive.

Use these XML tags	To do this
<code><jaas_config> </jaas_config></code>	Define a custom JAAS configuration. All JAAS configuration settings must be between these two tags.
<code><jaasConfiguration> </jaasConfiguration></code>	Define the name of your custom JAAS LoginModule. The value of this tag determines the tag name to use for the next tag. For example, if you create a custom configuration with the value <code>CustomConfig</code> , then you must use the tags <code><CustomConfig></code> and <code></CustomConfig></code> to define the list of adapters used.
<code><CustomConfig> </CustomConfig></code> <i>This is a user definable tag</i>	Define the list of <i>all</i> adapters that you want to use for authentication. Use semicolons between entries to specify multiple adapters. If the adapter name you list does not match a registered AdapterPool, then Get-Answers assumes the name is the logical name of a non-OAA LoginModule. Get-Answers attempts to authenticate users against each adapter you list. The values listed in this tag determine the tags names to use for each adapter. For example, if you create two adapters <code>adapter1</code> and <code>adapter2</code> , then you must use the tags <code><Adapter1></code> , <code></Adapter1></code> , <code><Adapter2></code> , and <code></Adapter2></code> to define your adapters.
<code><adapter1> </adapter1> <adapter2> </adapter2></code> <i>These are user definable tags</i>	Define the JAAS LoginModule settings for each adapter. Each adapter <i>must</i> have both <code><loginModule></code> and <code><controlFlag></code> tags defined for it.

Use these XML tags	To do this
<code><loginModule> </loginModule></code>	<p>Define the fully qualified class name of the JAAS LoginModule.</p> <p>This is <i>required</i> only when authenticating against non-OAA LoginModules (adapters). The default value is <code>com.peregrine.oaa.archway.security.OAALoginModule</code>.</p> <p>This is <i>optional</i> only when authenticating against Peregrine back-ends.</p>
<code><controlFlag> </controlFlag></code> This tag is <i>optional</i> .	<p>Define the authentication behavior of this LoginModule. The default value is REQUIRED.</p> <p>See <i>JAAS LoginModule control flags</i> on page 170 for a description of available options.</p>
<code><options> </options></code>	<p>Define the list of authentication options. Use semicolons between entries to specify multiple options. This is an <i>optional</i> setting for each JAAS LoginModule you use. See <i>JAAS configuration options</i> on page 173 for a description of available options.</p>

JAAS LoginModule control flags

The following table lists the possible settings for the `<controlFlag>` tag. A JAAS LoginModule can have one of four behaviors:

Control flag	Authentication behavior
REQUIRED	If the user cannot be authenticated against the adapter, the login fails. Whether it succeeds or fails, authentication continues to the next LoginModule in the list. This is the default behavior.
REQUISITE	If the user cannot be authenticated against the adapter, the login fails. If it succeeds, authentication continues to the next LoginModule in the list.

Control flag	Authentication behavior
SUFFICIENT	Authentication can proceed even if this LoginModule fails. If it succeeds, authentication does not continue to the next LoginModule in the list. If it fails, authentication continues to the next LoginModule in the list.
OPTIONAL	Authentication can proceed even if this LoginModule fails. Whether it succeeds or fails, authentication continues to the next LoginModule in the list.

Note: ControlFlag settings are case insensitive.

The overall authentication succeeds only if all Required and Requisite LoginModules succeed. If a Sufficient LoginModule is configured and succeeds, then only the Required and Requisite LoginModules prior to that Sufficient LoginModule need to have succeeded for the overall authentication to succeed. If no Required or Requisite LoginModules are configured for an application, then at least one Sufficient or Optional LoginModule must succeed.

By default, the controlFlag setting of all Get-Answers Web applications LoginModules is Optional. For most enterprises, this is the desired configuration.

The following table shows some sample scenarios and how the login process works.

Module Name	Status	Scenario 1	Scenario 2	Scenario 3
LoginModule1	required	pass	pass	fail
LoginModule2	sufficient	fail	fail	fail
LoginModule3	requisite	pass	pass	pass
LoginModule4	optional	pass	fail	fail
Final Authentication		pass	pass	fail

In Scenario 1, authentication succeeds even though LoginModule2 fails. This is because the Required loginModule takes precedence over the sufficient loginModule.

In Scenario 2, authentication succeeds because the loginModules that failed are only Sufficient and Optional.

Scenario 3 authentication fails because a loginModule with a status of Required failed.

JAAS configuration options

The following tables list the possible settings for the <options> tag.

Standard JAAS Options

The following table lists the standard JAAS options available for all adapters.

Option	Use	Description
debug=true	optional	Instructs a LoginModule to output debugging information. The OAALoginModule logs debugging information to stdout and not to archway.log .
tryFirstPass=true	optional	The first LoginModule in the list saves the password entered and this password is used by subsequent LoginModules. If authentication fails, the LoginModules prompt for a new password and repeats the authentication process.
useFirstPass=true	optional	The first LoginModule in the list saves the password entered and this password is used by subsequent LoginModules. If authentication fails, LoginModules do not prompt for a new password.
storePass=true	optional	Stores the password for the user being authenticated.
clearPass=true	optional	Clears the password for the user being authenticated.

Peregrine JndiLoginModule options

The following table lists the options available to custom JAAS LoginModules using the Peregrine JndiLoginModule.

Note: The Peregrine JAAS LoginModule `com.peregrine.oaa.security.JndiLoginModule` is modeled after Sun's `JndiLoginModule`. The main difference is that an RFC 2307 (NIS over LDAP) compliant schema is not required. User must have “uid” and “userPassword” properties defined.

Option	Use	Description
<code>user.provider.url</code>	required	<p>Use this option to provide the URL to the starting point in your directory service where you want to search for users.</p> <p>For example, <code>ldap://server/dc=peregrine,dc=com</code></p> <p>Note: This option corresponds to the Java constant <code>Context.PROVIDER_URL</code>.</p>
<code>security.principal</code>	optional	<p>Use this option to specify which directory service user you want to use to authenticate non-anonymous queries of your directory service. Use the DN of the directory service user. For example, <code>uid=user,dc=peregrine,dc=com</code></p> <p>Tip: To prevent user passwords from being visible to users, you should only set this option if you are using a directory server such as IPlanet where user passwords are SHA hashed by default.</p> <p>Note: This option corresponds to the Java constant <code>Context.SECURITY_PRINCIPAL</code>.</p>

Option	Use	Description
security.credentials	optional	<p>Use this option to define the password for the <code>security.principal</code> user. This option should only be used in conjunction with the <code>security.principal</code> option.</p> <hr/> <p>Important: If you are using a simple security authentication protocol, then this password may be passed as plain text.</p> <hr/> <p>Tip: To safeguard this password, either enable SSL (set the <code>security.protocol=ssl</code> option) or use an <code>security.authentication</code> that protects passwords.</p> <p>Note: This option corresponds to the Java constant <code>Context.SECURITY_CREDENTIALS</code>.</p>
security.protocol	optional	<p>Use this option to enable or disable an SSL connection between the <code>JndiLoginModule</code> and your directory server. This option has two possible values:</p> <ul style="list-style-type: none"> ■ <code>simple</code> (Default setting) ■ <code>ssl</code> <p>Note: This option corresponds to the Java constant <code>Context.SECURITY_PROTOCOL</code></p>
security.authentication	optional	<p>Use this option to enable or disable anonymous binding to your directory service. Typically, this option has one of two values:</p> <ul style="list-style-type: none"> ■ <code>none</code> (Default setting) ■ <code>simple</code> <p>Note: If you do not specify a value for <code>security.principal</code> then <code>security.authentication</code> defaults to a value of <code>none</code>. Likewise, if you set <code>security.authentication</code> to <code>simple</code> but <code>security.credentials</code> is omitted or has zero length, then <code>security.authentication</code> resets to <code>none</code>.</p> <p>Note: This option corresponds to the Java constant <code>Context.SECURITY_AUTHENTICATION</code>.</p>

Option	Use	Description
<code>user.search.scope</code>	optional	<p>Use this option to specify the number of levels to descend when searching for the user being authenticated by <code>user.provider.url</code>. This value must be an integer. The default value is 1.</p> <p>Note: This option corresponds to the Java constant <code>SearchControls.ONELEVEL_SCOPE</code>.</p>
<code>group.provider.url</code>	optional	<p>Use this option to provide the URL to the starting point in your directory service where you want to search for groups.</p> <p>For example, <code>ldap://server/dc=peregrine,dc=com</code></p> <p>Note: This option corresponds to the Java constant <code>Context.PROVIDER_URL</code>.</p>
<code>group.search.scope</code>	optional	<p>Use this option to specify the number of levels to descend when searching for a group. This option should only be used with <code>group.provider.url</code>. This value must be an integer. The default value is 1.</p> <p>Note: This option corresponds to the Java constant <code>SearchControls.ONELEVEL_SCOPE</code>.</p>
<code>group.search.objectClass</code>	optional	<p>Use this option to specify the name of the LDAP group objectClass. Valid values are:</p> <ul style="list-style-type: none"> ■ <code>groupOfNames</code> (Default value) ■ <code>groupOfUniqueNames</code>. ■ <code>groupOfUrls</code> <p>Note: Either <code>groupOfNames</code> or <code>groupOfUniqueNames</code> can be used to define static groups in LDAP, but they may not be used together.</p> <p>If you choose the <code>groupOfUrls</code> option, then you are configuring dynamic groups. No additional configuration settings are required to recognize dynamic groups.</p>
<code>storeIdentity=true</code>	optional	<p>Use this option to store a reference to the User being authenticated.</p>
<code>clearIdentity=true</code>	optional	<p>Use this option to clear a reference to the User being authenticated.</p>

Example: Defining an LDAP custom configuration

The following XML code is an example of how to define a loginModule to authenticate users against an LDAP directory service.

Note: LDAP is not an adapter and does not imply any other functionality.

```
<jaas_config>
  <jaasConfiguration>myConfig</jaasConfiguration>
    <myConfig>ldap</myConfig>

    <ldap>
      <loginModule>
        com.peregrine.oaa.security.JndiLoginModule
      </loginModule>
      <options>
        user.provider.url=ldap://server/dc=peregrine,dc=com;
        group.provider.url=ldap://server/dc=peregrine,dc=com
      </options>
    </ldap>
  </jaas_config>
```

Standard Sun Microsystems JAAS configuration

The standard JAAS configuration option authenticates users against the Sun Microsystems formatted JAAS configuration. To enable the standard JAAS configuration, you must edit the local.xml file and add the following lines:

```
<jaas_config>
  <useStandardJAASConfiguration>true</useStandardJAASConfiguration>
</jaas_config>
```

If you choose to use the standard JAAS configuration, then you must also do one of the following two things:

- Specify the appropriate JAAS command line options when the container is started
- or–
- Configure the java.security file in \$JAVA_HOME/jre/lib/security for JAAS.

Command line options

The command line properties required for use of the standard file-based configuration are as follows:

```
java -classpath <list of jars> \  
-Djava.security.manager \  
-Djava.security.policy==java2.policy \  
-Djava.security.auth.policy==jaas.policy \  
-Djava.security.auth.login.config==jaas.config \  
<MyMainClass>
```

For *<list of jars>*, enter the list of jars used by your JAAS-enabled Java application.

For *<MyMainClass>*, enter the fully qualified class name of the Java main program class.

Integrated Windows Authentication

Windows Integrated Authentication (known as NT/Challenge Response in previous versions of Windows) is one of the ways Windows facilitates the authentication of users on a Web server. The process consists of a secure handshake between Internet Explorer (IE) and the Internet Information Server (IIS) Web server. The handshake lets the Web server know exactly who the user is, based on how they logged in to their workstation. This allows the Web server to restrict access to files or applications based on who the user is. Applications running on the Web server can use this information to identify users without requiring them to log in.

Get-Answers uses Integrated Windows Authentication as follows:

- The user logs in to a Windows XP/2000/NT workstation.
- The user starts the IE browser and navigates to the `login.asp` page.
- IE automatically sends user authentication information to IIS. The user's password is not transferred, but the Integrated Windows Authentication handshake between IE and IIS is enough for the server to recognize the user.
- The Web application login automatically detects the user by using the Integrated Windows Authentication/IIS server data.
- The user is logged in without requiring that a name and password be entered.

During this process, the back-end database authenticates and impersonates the Windows user with each of its adapters.

The following circumstances are exceptions to the normal Integrated Windows Authentication login process:

- The Windows user has already registered with a back-end database adapter. When this occurs, Get-Answers asks the user to register and enter profile information. Get-Answers then lets the user log in and stores this information for future login attempts.
- The Windows user name is not already registered as an Administrator in the back-end system. When this occurs, the web application does not proceed with automatic login. The user is presented with another login screen and is asked to verify their password. This step is an added security measure to prevent a user from accidentally logging in with administrative rights.

Setting up Integrated Windows Authentication

This section describes how to configure Get-Answers to use IIS for Integrated Windows Authentication while using Apache as the primary Web server. You can also follow these instructions if you use IIS as your primary Web server.

It is a seven-step process:

- Step 1** Verify that all users have an Operator record in the appropriate back-end database. See *Creating an Operator record* on page 180.
- Step 2** Install and configure Get-Answers with Apache and Tomcat. See *Preparing to configure Integrated Windows Authentication* on page 180.
Note: Tomcat/Apache is the preferred configuration for Get-Answers.
- Step 3** Set Web server properties for the `login.asp` file. See *Setting Web server properties for the login.asp file* on page 180.
- Step 4** Set Web server properties for the `e_login_main_start.asp` file. See *Setting Web server properties for the e_login_main_start.asp file* on page 182.
- Step 5** Set Web server properties for the `loginverify.asp` file. See *Setting Web server properties for the loginverify.asp file* on page 185.

- Step 6** Set the **Require Windows NT Challenge/Response Authentication** parameter, and optionally the **Default User Login Name** and **Default Login User Password** parameters from the Get-Answers administration page. See *Setting the Admin parameters* on page 186.
- Step 7** Optionally, define the **LogoutURL** from the Get-Answers administration page. This step is necessary when Get-Answers and IIS reside on different servers. See *Setting up the LogoutURL* on page 187.

The following procedures illustrate how to setup Integrated Windows Authentication using Windows 2000 as an example. If you are using Windows XP, the overall procedure is the same. The IIS Management Console is called Internet Information Services.

Creating an Operator record

All users must have a back-end database Operator record. Contact your AssetCenter or ServiceCenter administrator to verify that users have Operator records. Create an Operator record as needed.

Preparing to configure Integrated Windows Authentication

Note: If you are not using the preferred Tomcat/Apache configuration, skip this section.

- 1 Install and configure Get-Answers with Apache and Tomcat, and verify that you can log in through `login.jsp`.
- 2 On a server running IIS, create a virtual directory named `oaa`.
This virtual directory must have read access and permission to run scripts.
- 3 From the Get-Answers deployment directory, copy the following files to the `oaa` virtual directory on the IIS server:
 - `login.asp`
 - `loginverify.asp`
 - `e_login_main_start.asp`

The default Get-Answers deployment directory is:

`C:\Program Files\Peregrine\Common\Tomcat4\webapps\oaa`

Setting Web server properties for the login.asp file

Note: If you are using IIS for your Web server, go directly to step 3.

- 1 On the IIS server, edit `login.asp` using a text editor.

Edit <FORM... action...> and change it from `login.jsp` to the absolute URL of `login.jsp` on the Apache server.

For example, change from:

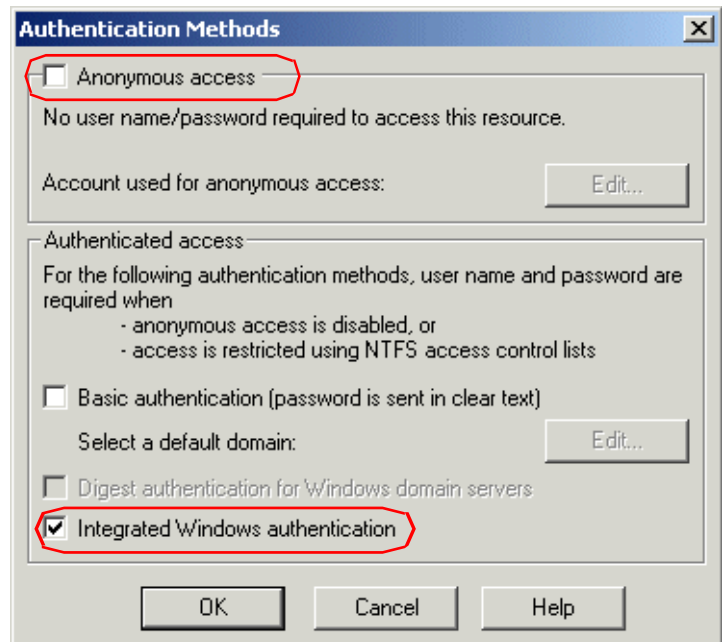
```
<FORM name="f" action="login.jsp" method="post">
```

to:

```
<FORM name="f" action="
"http://<apacheserver.mycompany.com>/oaa/login.jsp" method="post">
```

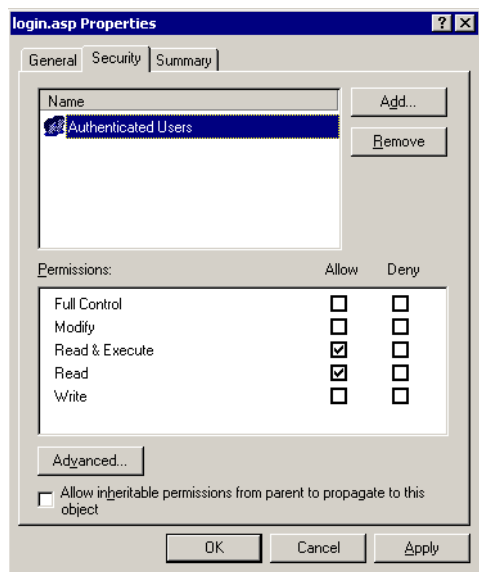
- 2 Open the IIS Management Console (**Start>Programs>Administrative Tools>Internet Information Services**).
- 3 Click on the `oaa` virtual directory.
- 4 Right-click on `login.asp` and select **Properties**.
- 5 Select the **File Security** tab.
- 6 Click **Edit** in the **Anonymous Access and Authentication Control** section and set the permissions as follows:
 - a Disable **Anonymous access**.
 - b Require **Integrated Windows authentication**.

Clear the Anonymous access check box.



Select the Integrated Windows authentication check box.

- 7 Click OK on all windows displayed until you return to the Microsoft Management Console.
- 8 From Windows Explorer, update the following properties to **login.asp**.
 - a Add the **Authenticated Users** group to the list of authorized users.
 - b Grant the following **Permissions** to the Authenticated Users group:
 - **Read & Execute** – Allow
 - **Read** – Allow



Setting Web server properties for the e_login_main_start.asp file

Note: If you are using IIS for your Web server, go directly to step 3.

- 1 On the IIS server, edit e_login_main_start.asp using a text editor. Edit <FORM... action...> and change it from e_login_main_start.do to the absolute URL of e_login_main_start.do on the Apache server.

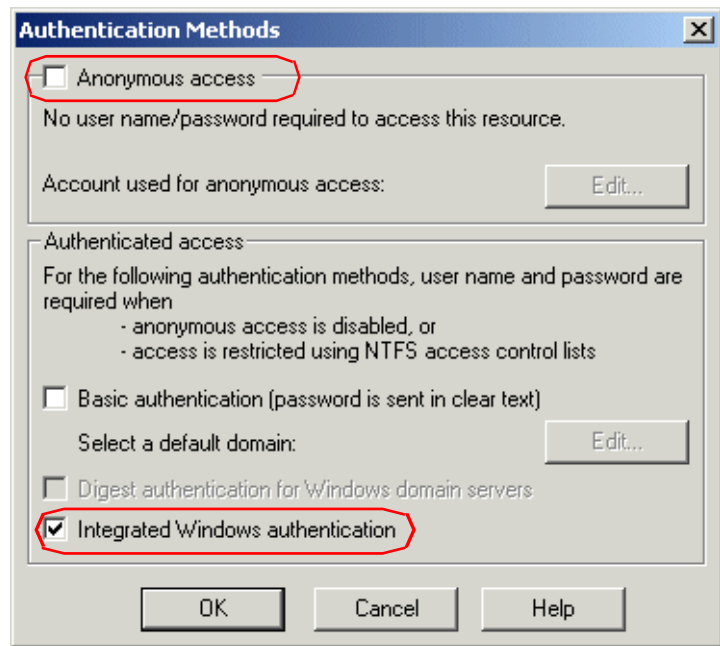
For example, change from:

```
<FORM name="f" action="e_login_main_start.do" method="post">
to:
```

```
<FORM name="f" action="http://<apacheserver.mycompany.com>
/aaa/e_login_main_start.do" method="post">
```

- 2 Open the IIS Management Console (Start>Programs>Administrative Tools>Internet Information Services).
- 3 Click on the oaa virtual directory.
- 4 Right-click on e_login_main_start.asp and select **Properties**.
- 5 Select the **File Security** tab.
- 6 Click **Edit** in the **Anonymous Access and Authentication Control** section and set the permissions as follows:
 - a Disable **Anonymous** access.
 - b Require **Integrated Windows** authentication.

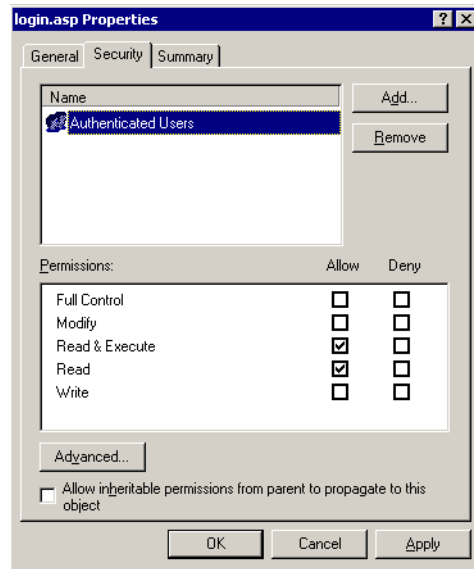
Clear the Anonymous access check box.



Select the Integrated Windows authentication check box.

- 7 Click **OK** on all windows displayed until you return to the Microsoft Management Console.
- 8 From Windows Explorer, update the following properties to e_login_main_start.asp.
 - a Add the **Authenticated Users** group to the list of authorized users.
 - b Grant the following **Permissions** to the **Authenticated Users** group:
 - **Read & Execute** – Allow

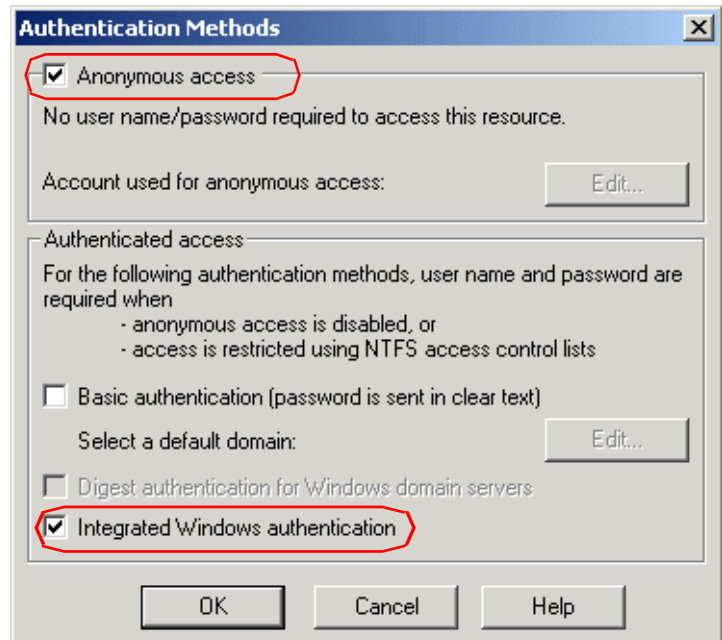
■ Read – Allow



Setting Web server properties for the loginverify.asp file

- 1 Open the IIS Management Console (Start>Programs>Administrative Tools>Internet Information Services).
- 2 Click on the oaa virtual directory.
- 3 Right-click on loginverify.asp and select **Properties**.
- 4 Select the **File Security** tab.
- 5 Click **Edit** in the **Anonymous Access and Authentication Control** section.

Select the Anonymous access check box.



Select the Integrated Windows authentication check box.

- 6 Verify that **Anonymous access** and **Integrated Windows authentication** have a check.
- 7 Click **OK** on all windows displayed until you return to the Microsoft Management Console.
- 8 Close the Management Console.

Setting the Admin parameters

You must set the **Require Windows NT Challenge/Response Authentication** parameter to Yes if you want only users who have a Windows account to log in. Users without Windows authentication can still have login capabilities by assigning a Default Login User Name.

Warning: The default login user has whatever capabilities you assign in the ServiceCenter or AssetCenter back-end. When you enable this feature, anyone can log in. Assign minimal user rights to this user.

To set Windows NT Challenge/Response Authentication:

- 1 Open a Web browser.
- 2 Enter the following URL: `http://<webserver>/<oaa>/admin.jsp` in the browser address field (where `<webserver>` is the name of your Web server and `<oaa>` is the name of the virtual directory created during installation).
- 3 Login using the administrator name and password.
- 4 From the Administration Home page, click **Settings**.

Select the Yes option in Require Windows NT Challenge/Response Authentication to allow only Windows users to log in.

The screenshot shows the 'Admin Settings' web interface. On the left is a navigation tree with 'Settings' selected. The main content area is a table with configuration parameters and their descriptions. The 'Require Windows NT Challenge/Response Authentication' row is circled in red, showing the 'Yes' radio button selected.

Parameter	Description
Logout URL:	Destination URL displayed when a user logs off of system.
Server URL:	Link back to server. Replace localhost with the server name. Applications may append at run time the targeted jsp page.
Message URL Prefix:	Defines the http domain used to build URL references with coded messages.
Help URL Prefix:	Defines the URL Prefix used to access help forms. When set, a help URL is generated in the form {HelpURLPrefix}?form={module}_{activity}_{form}&language={userlocale}, where {HelpURLPrefix} is a configuration property. If {HelpURLPrefix} is undefined, then the URL is generated in the form help/{userLocale}/e_{module}_{activity}_{form}.html.
Loginverify.asp URL prefix:	Enter URL prefix for loginverify.asp if IIS is on a different server than OAA. For example: <code>http://iisserver.mycompany.com/oaa/</code>
Require Windows NT Challenge/Response Authentication:	Set to true to allow only users who are preauthenticated by Windows to log in. You must configure NT Challenge/Response authentication as described in the setup guide before enabling this option. Set this together with the Logout URL option. Click for default [No]
Default Login User Name:	Optional default user name, having minimal privileges, to use to log into back-end systems when the initial NT Challenge/Response login attempt fails. Note: Enabling this setting could pose a security threat; assign a default user with very minimal access rights to backend systems. Click for default [1]
Default Login User Password:	The password for the Default Login User Name. It is not necessary to provide a password for the Default Login User Name unless the user name has been assigned an actual password to the backend systems.

- 5 From the **Common** tab, set the **Require Windows NT Challenge/Response Authentication** parameter to Yes.
- 6 To allow users without Windows authentication to login, assign a Default Login User Name, and optionally a password.
- 7 Click **Save**, then click **Reset Server**.

Setting up the LogoutURL

Note: This step is necessary when Get-Answers and IIS reside on different servers.

- 1 From the Administration home page (see *To set Windows NT Challenge/Response Authentication*: on page 186), click **Settings**.
- 2 From the **Common** tab, set the **LogoutURL** setting to the URL you want users to go to if Integrated Windows Authentication fails or is not possible due to the user's current browser.
- 3 Click **Save**, then click **Reset Server**.

Testing the settings

Log in to your Peregrine Web application to make sure the access permissions are set correctly. The Integrated Windows Authentication settings are activated when you log in through a special login page named `login.asp`. Accessing your applications through the standard `login.jsp` page results in the users needing to log on as usual.

To test the settings:

- 1 Open a Web browser.
- 2 Enter the following URL: `http://<webserver>/<oaa>/login.asp` in the browser address field (where `<webserver>` is the name of your Web server and `<oaa>` is the name of the virtual directory created during installation).
- 3 Verify that access to Get-Answers is what you expected based on the settings you chose for the `login.asp` and `loginverify.asp` files.

Integrating with single sign-on tools

You can integrate Get-Answers with a single sign-on tool such as SiteMinder to eliminate displaying the Get-Answers login screen. When you integrate with a single sign-on tool, Get-Answers users browse to a special URL that obtains their user information from the sign-on tool and then automatically logs them in if the sign-on tool validates them. The following steps are for integrating Get-Answers with a third-party single sign-on tool. If you want to use Integrated Windows Authentication as your single sign-on tool, refer to *Integrated Windows Authentication* on page 178.

To integrate with a single sign-on tool:

- 1 Choose or create one user record for each single sign-on user you want to access Get-Answers. Each user record must have a password and a list of capability words or user rights.

Important: The back-end database user record is required to determine what portions of the Get-Answers interface the user can access.

- 2 Open a text editor such as NotePad.
- 3 Create a new JSP file to be the target of your automatic login URL.

You can use the following code as a template:

Add JSP code here to obtain the user name of the person that the single sign-on tool has authenticated _____	<pre><%@ include file="jspheader.jsp" %> <% // Add JSP code that obtains proper user name from // the third party single-sign on tool // ... // Replace "user" with the user name obtained above String sUser = "user"; // Turn on OAA pre-authentication user.setPreAuthenticated(true); %> <HTML> <BODY> <FORM name="f" action="login.jsp" method="post"> <INPUT type="hidden" name="loginuser" value="<%=sUser%>" /> </FORM> </BODY> </HTML> <SCRIPT LANGUAGE="JavaScript"> self.document.forms[0].submit() </SCRIPT></pre>
Replace the value _____ "user" with the user name obtained from your single sign-on tool	

- 4 Add any necessary JSP code to query your single sign-on tool for the name of the user who has been pre-authenticated.

Typically, these tools use HTTP headers to submit this information. See your single sign-on tool API documentation for details.

- 5 Save the file as `autologin.jsp` in your application server's presentation folder. For example:

C:\Program Files\Peregrine\Common\Tomcat4\webapps\oaa\autologin.jsp

Note: The name you choose for the JSP file will be the file name required in the URL.

Testing access to Get-Answers from a single sign-on tool

You can use the following steps to test access to Get-Answers from your single sign-on tool.

To test your single sign-on settings:

- 1 Login to your single sign-on tool.
- 2 Open a browser and go to the following URL:

`http://<server_name>/oaa/autologin.jsp`

If you configured the login settings correctly you will be authenticated and redirected automatically to the Get-Answers home page.

Note: If you saved the automatic login page with a different file name, then use that file name instead of `autologin.jsp`.

Contact-based authentication

The following method describes an alternate authentication scheme that automatically verifies Windows users as ServiceCenter contacts.

You can configure Get-Answers to automatically log in specific groups of authenticated Windows users as one or more pre-defined Operators in ServiceCenter. Each group of Windows users has its own login page.

- Step 1** Choose or create one Operator record in ServiceCenter for each group of Windows users you want to authenticate. See *Creating an Operator record in ServiceCenter* on page 190.
- Step 2** From the Windows domain server, add a Windows group for each Operator that you defined in step 1. Refer to your Windows documentation for more information on adding groups. See *Adding groups* on page 191.
- Step 3** Create a login ASP file for each Operator defined in step 1. See *Configuring the login ASP file* on page 191.
- Step 4** Configure each login ASP file to be exclusive to each Windows group defined in step 2. See *Setting properties for the login ASP file* on page 192.
- Step 5** Edit local.xml in <application server>\oaa\WEB-INF to define the passwords for each Operator defined in step 2. See *Editing the local.xml file* on page 194.

Creating an Operator record in ServiceCenter

Choose or create one Operator record for each group of users or role you want to access Get-Answers. Each Operator must have a password and a list of capability words. For example, you can define one Operator with default access (`scdefault`) and one Operator with manager access (`scmgr`). Refer to your ServiceCenter documentation for more information on adding Operator records.

The following procedures describe how to use `scdefault` and `scmgr` as the Operators.

Using Operator records in ServiceCenter:

- 1** Create two Operator records: `scdefault` and `scmgr`.
Refer to your ServiceCenter documentation for information on adding Operator records.

- 2 Add the Get-Answers capability words you want users assigned to this Operator to have. For example:

Operator	Capability words
scdefault	getit.service getit.personalization.default
scmgr	getit.service getit.employee getit.itmanager getit.personalization.default

Note: Each Operator will use its own login page.

In this example, users who log in to `logindefault.asp` have the capabilities of the `scdefault` Operator in ServiceCenter. Users who log in to `loginmgr.asp` have the capabilities of the `scmgr` Operator in ServiceCenter.

- 3 Assign a password to each Operator.

Note: The password must match the password defined in *Editing the local.xml file* on page 194.

Adding groups

You must have an equivalent Windows group for each Operator that you want to authenticate. For example:

Operator	Suggested group
scdefault	Authenticated Users (default Windows group)
scmgr	Managers (created on domain server)

Refer to your Windows documentation for adding groups to Windows.

Configuring the login ASP file

You must configure or create a separate login ASP file for each Operator you define (see *Creating an Operator record in ServiceCenter* on page 190). Each file needs a unique name.

Two sample login ASP files, `logindefault.asp` and `loginmgr.asp` are in the Get-Answers deployment directory: `<application server>\oaa`

To configure the login ASP file:

- 1 Create a unique login file for each Operator.
For example, create `logindefault.asp` for `scdefault` and create `loginmgr.asp` for `scmgr`.
 - a Copy `logindefault.asp` from the deployment folder:
`<application server>\oaa`
 - b Paste the file in the same folder and rename the copied file.

Note: Whatever file name you choose becomes part of the URL users enter to access Get-Answers. For example, if the file name is `mylogin.asp`, the URL is: `http://yourhostname/oaa/mylogin.asp`.
- 2 Edit the value of the OPERATOR form input to match the Operator you defined in *Creating an Operator record in ServiceCenter* on page 190.

```

...
<FORM name="f" action="login.jsp" method="post">
  <INPUT type="hidden" name="AUTH_TYPE" value="<%=sType%>" />
  <INPUT type="hidden" name="AUTH_USER" value="<%=sUser%>" />
  <INPUT type="hidden" name="AUTH_KEY" value="<%=sKey%>" />
  <INPUT type="hidden" name="OPERATOR" value="scdefault" />
</FORM>
...

```

The value of the OPERATOR must match the Operator name.

- 3 Save and close the file.

Setting properties for the login ASP file

You must configure each login ASP file to be exclusive to each Windows group. This requires changing the authentication method in IIS and setting the file security properties in Windows.

To change the authentication method in IIS:

- 1 Open the IIS Management Console (Start > Programs > Administrative Tools > Internet Information Services).
- 2 Navigate to the `oaa` virtual directory.
- 3 For each Operator, navigate to the ASP file that you created in *Configuring the login ASP file* on page 191.
For example, navigate to `logindefault.asp` for `scdefault`; navigate to `loginmgr.asp` for `scmgr`.

- 4 Right-click on the file and select **Properties**.
- 5 Select the **File Security** tab.
- 6 Click **Edit** in the **Anonymous Access and Authentication Control** section and set the permissions as follows:
 - a Disable **Anonymous** access.
 - b Require **Integrated Windows** authentication.

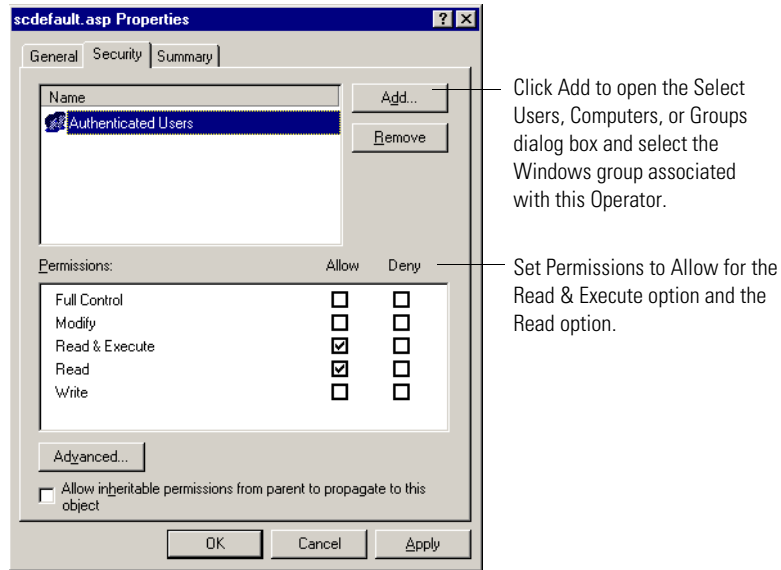


- 7 Click **OK** on all windows displayed until you return to the Microsoft Management Console.

To set the file security properties in Windows:

- 1 Open Windows Explorer.
- 2 Browse to your deployment folder: <application server>\oaa
- 3 Update the following login ASP properties.
 - a Right-click on your login ASP file; for example, scdefault.asp, and click **Properties**.

- b Add the user group associated with this Operator; for example, **Authenticated Users**.



- c Grant the following **Permissions** to the **Authenticated Users** group:
- Read & Execute – Allow
 - Read – Allow
- d Click **OK**.
- 4 Repeat step 3 for each login ASP file.

Editing the local.xml file

You must identify the password for each Operator that you defined in the local.xml file. This file is located at:

<application server>\oaa\WEB-INF\local.xml.

To edit the local.xml file:

- 1 Using a text editor, edit local.xml.

The default location is:

C:\Program Files\Peregrine\Common\Tomcat4\webapps\oaa\WEB-INF.

- 2 Add an XML entry for each Operator.

The tag has the format: <[operator name]password>

For example, for `scmgr` and `scdefault`, add the following inside the <settings> ... </settings> tags:

```
<scmgrPassword>password1</scmgrPassword>
<scdefaultPassword>password2</scdefaultPassword>
```

Important: The password must match the Operator password in ServiceCenter.

- 3 Restart your application server for your changes to take effect.

Creating an alternate login page

If you do not want to use the default Peregrine OAA login page, you can create your own login page that authenticates users and redirects them to the proper start page. Creating an alternate login page requires two basic steps:

- Step 1** Create a login Web page with the necessary authentication parameters. See the following section, *Creating a login Web page*.
- Step 2** Edit the `archway.xml` to specify the HTTP authentication method you want to use. See *Specifying an alternate authentication method* on page 197.

Creating a login Web page

Your custom login web page can be any HTML form that prompts for the following required parameters:

- Username
- Password

In addition, you can include optional login parameters such as:

- Display Language and Locale
- Time format
- Theme

A sample HTML login form, `login_sample.htm` is in the OAA deployment folder of your application server:

```
<application server>\WEB-INF\oaa\
```

Customize this sample HTML form using the following guidelines:

- Whatever custom login file you create becomes part of your login URL. For example, if you create a custom page called `my_login.htm`, then the login URL is `http://<server>:<port>/oaa/my_login.htm`
- You must specify the `basicauth` servlet in the form action. For example, `action="http://<server>:<port>/oaa/servlet/basicauth"`
- Users who have the `getit.portal` capability word see the `e_portal_home_start.do` home page if successfully authenticated
- Users who do *not* have the `getit.portal` capability word see the `e_home_main_start.do` home page if successfully authenticated
- Users who fail to be successfully authenticated see the page specified in the `_failURL` value
- The `basicauth` servlet does not encrypt usernames and passwords during login. You must enable HTTPS if you are concerned about password security on your intranet.
- If no URL is specified in the form action, then authenticated users are redirected to `http://<server>:<port>/oaa/login.jsp` where they see either `e_portal_home_start.do` or `e_home_main_start.do` depending on their login capability words.
- There are no specific Administration page settings needed to set up a custom login page. You must define all login parameters in your custom login page.
- If you want to display a specific OAA page at login, you can specify the page in the form action URL. For example, the value `action="http://<server>:<port>/oaa/servlet/basicauth/e_home_main_start.do"` displays the non-portal version of the Peregrine OAA home page.
- The following login parameters are available:

Login parameters	Description
<code>loginuser</code>	This is a required login parameter specifying the user name. You must specify a form input for this parameter.
<code>loginpass</code>	This is a required login parameter specifying the login password. You must specify a form input for this parameter.
<code>_locale</code>	This is an optional login parameter specifying the user's locale and regional display settings.

Login parameters	Description
_timezone	This is an optional login parameter specifying the user's timezone.
_theme	This is an optional login parameter specifying which theme should be displayed in the Peregrine OAA Portal

Specifying an alternate authentication method

By default, Peregrine OAA uses HTTP basic authentication provided by the `HttpBasicAuthenticationManager` class. If you create a custom login page, you need to specify the alternate authentication method in the `archway.xml` file.

To specify an alternate HTTP authentication method:

- 1 Stop your application server.
- 2 Using a text editor, open the `archway.xml` file located at:

```
<application server>\webapps\oaa\WEB-INF\default.
```

- 3 Edit the line containing:

```
<httpauthclass ...>HttpBasicAuthenticationManager</httpauthclass>
```

- 4 Change the value `HttpBasicAuthenticationManager` to `HttpAlternateAuthenticationManager`.
- 5 Save the file.
- 6 Modify the `web.xml` file.

You will need to enable the `AuthController` servlet to establish a proxy for HTTP basic authentication.

- a Using a text editor, open the `web.xml` file located at:

```
<application server>\webapps\oaa\WEB-INF.
```

b Add the following lines at the end of the last `<servlet>` definition:

```
<servlet>
  <servlet-name>AuthController</servlet-name>
  <display-name>AuthController</display-name>
  <description>A controller (decorator) servlet that can be used to enable
  configurable auth protection of any resource.</description>

  <servlet-class>com.peregrine.oaa.archway.AuthControllerServlet
</servlet-class>
  <load-on-startup>2</load-on-startup>
</servlet>

<servlet-mapping>
  <servlet-name>AuthController</servlet-name>
  <url-pattern>/servlet/basicauth/*</url-pattern>
</servlet-mapping>
<servlet-mapping>
  <servlet-name>AuthController</servlet-name>
  <url-pattern>/servlet/auth/*</url-pattern>
</servlet-mapping>
```

c Save the file.

7 Restart your application server.

Warning: Changing the HTTP authentication setting to the Alternate Authentication Manager exposes queries (including login names and passwords) in the URL. If you want to protect URL queries, then you must restrict access to this information through your Web server.

9 Customizing Get-Answers

CHAPTER

This chapter discusses how to customize some of the features of Get-Answers. You can modify the stop word list, modify the search engine dictionaries, customize the text editor (edit-on Pro), and customize the spelling checker used with the editor.

Topics in this chapter include:

- *Understanding the search engine Stop Words list* on page 200
- *Using search engine dictionaries* on page 203
- *Setting up custom dictionaries* on page 205
- *Customizing edit-on Pro* on page 212
- *Customizing the edit-on Pro spelling checker* on page 219

Understanding the search engine Stop Words list

Stop words are function words in the English language, such as *a*, *the* and *and*. Get-Answers contains a standard Stop Words file (`rw_english.slx`) that includes a list of these words.

Note: You can see the Get-Answers Stop Words list. To do so, open the file `rw_english.slx` in a text editor such as Notepad.

This section explains the following:

- The exceptions to the Stop Words list. (See *Stop Words list exceptions* on page 200.)
- How words you add or remove from the Stop Words list affect searching in Get-Answers. (See *New and deleted Stop words* on page 201.)
- How to add or remove Stop words from the Stop Words list. (See *Modifying the Stop Words list* on page 202.)

Stop Words list exceptions

Get-Answers uses the Stop Words file to identify and remove common words from indexes and user queries. This means that Get-Answers won't look for these common words when searching documents for content matches.

Stop words are removed from indexes and queries with the following exceptions:

- During query processing for an Advanced Search, if the query type is Boolean, the words AND, OR, NOT, and BUT are not removed (since they are recognized as Boolean operators).
- Stop words are skipped during indexing only if the word in the input file is exactly the same word in the stop words file. (For example, if "in" is in the stop words file, "INS" is still indexed).

- Stop words in a particular database field are not removed if the `NO_STOP_WORDS` flag is set in the configuration file (`rware.cfg`) for that field. For example, the `NO_STOP_WORDS` flag is set for the file name and the file extension fields, so that a file named ‘begin.out’ would not be reduced to a single period if the Stop words ‘begin’ and ‘out’ were removed.
- Stop words contained within idioms (for example, “by” and “all” within “by all odds” or the idiom “to be”) are not removed as long as the idiom exists in the dictionary. If an idiom with Stop words is indexed, an indicator for the idiom is indexed, not the individual words contained in the idiom. This makes idioms independent of the Stop words file. You can, however, set up entire idioms in the Stop words file (stop idioms) for any idioms contained in an indexing dictionary. This removes the idiom from the indexing and query processes.

New and deleted Stop words

When you add a Stop word to the Stop Words list, Get-Answers does not use the Stop word for searching. When you delete Stop words from the Stop Words list, Get-Answers does use the Stop word in searching.

This section explains how Get-Answers treats words that you add or remove from the Stop Words list.

When you add Stop words, keep the following in mind:

- These Stop words are not removed from the existing indexes. However, they are removed from any queries, so their presence in the indexes does not influence searching.
- Stop words you add are removed from all queries the next time the query program is started.
- New Stop words are not included in any future document indexes you create.

When you remove stop words from the Stop Words file, keep the following in mind:

- These Stop words are not automatically added back into the document indexes, and queries on existing documents won’t find those words. To add former stop words back into existing document indexes, you must delete the index files and then re-index the library. (See *To delete the index files and re-index the library*: on page 202)

- Queries on deleted stop words do not retrieve any documents indexed prior to the change. (A query using the removed stop words would not retrieve anything because the indexes for existing documents are still missing those words.)
- Stop words you have deleted from the Stop Words list are included in any future document indexes you create.

To delete the index files and re-index the library:

- 1 Go to **Start > Programs > Get-Answers Search Engine > System Utilities Menu.**

```

----- GETANSWERS SEARCH ENGINE SYSTEM UTILITIES -----
Choose a menu option:
1. [ Exit this program ]
2. Choose a working directory
   Currently working with: C:\getanswers\Peregrine
3. Administration Servers - Start/Stop/Restart/Status
4. Search and Indexing Servers - Start/Stop/Restart/Status
5. Log Files and Temporary Files - Display or delete them
6. Indexing and index utilities
7. Query Program - Standalone <SQuery>
8. Query Program - Client/Server <CLSqry>
9. RDBMS scripts and utilities
10. Profiling utilities
11. System and server tests
12. System recovery utilities [Use BEFORE restarting servers]
13. Licensing checks
14. GetAnswers Search Engine Internet Spider utilities
>

```

- 2 Choose option 6 - Indexing and Index Utilities.
- 3 Choose option 4 - Index RDBMS Records.
- 4 Choose option 3 - Index all RDBMS Records in your library.
- 5 Enter KMLib. This is the knowledge management library you want to index.
- 6 Enter 1 - Yes to update the index.
- 7 Choose option 1 - Return to previous menu.
- 8 Choose option 1 - Return to previous menu.
- 9 Choose option 1 - Exit this program.

Modifying the Stop Words list

Before you make changes to the Stop Words file, read the following syntax rules.

- One stop word is allowed per line.
- Stop words must appear in all uppercase letters.

- The stop words require no specific order.
- “Stop idioms” are allowed, as long as the idiom exists in an indexing dictionary. Words in the idiom must be separated by a single space. (Multiple spaces or tabs are not allowed).
- Stop words must be spelled exactly as they appear in the text because they are not removed from the processing pipeline until after morphological analysis has taken place. For example, if “begin” is a stop word, you might also want to include “beginning,” “began,” and “begins.”
- Blank lines in the file are allowed.
- Leading spaces are not allowed. Trailing spaces are automatically removed.

Important: Consider saving a copy of the original Stop Words file before you change it. The `rw_english.slx` file is a standard ASCII text file. You can edit it using any word processing program or ASCII text editor.

To modify the stop words list:

- 1 Open the `rw_english.slx` file in a text editor. The file is located in the `\getanswers\resource\rw_english` directory.
- 2 Make the desired additions or deletions to the file using the guidelines mentioned above.
- 3 Save the file.

Using search engine dictionaries

Get-Answers uses the dictionary during both indexing and queries. The dictionary enables Get-Answers to perform “concept” searching, which means that it automatically finds words related to query terms.

Get-Answers provides a baseline English dictionary. This section describes how to create a custom dictionary of your own to use along with the English dictionary for indexing and/or querying.

The baseline English dictionary was compiled from the following electronic sources:

- American Heritage® Dictionary of the English language, Third Edition
© Copyright 1992 by Houghton Mifflin Company
- Enhanced Roget's US Electronic Thesaurus
© Copyright 1995 by Inso Corporation
- Enhanced Roget's UK Electronic Thesaurus
© Copyright 1995 by Inso Corporation
- WordNet 1.5
© Copyright 1991, 1993, 1995 by Princeton University

A Get-Answers “dictionary” consists of the five files listed below, contained in a single directory:

- **semantic.db** — Semantic database of meanings and the words related to each one
- **irreg.db** — Lists of related words with irregular morphology or alternate spellings
- **semantic.xrf** — Concept cross-reference network of the **semantic.db** file
- **irreg.xrf** — Concept cross-reference network of the **irreg.db** file
- **expand.wgt** — Weights for words expanded via the semantic database

Each dictionary's files are totally independent from those of any other dictionary.

Updating indexes for search engine dictionary changes

If you edit a dictionary that you used for indexing, Peregrine recommends that you re-index the affected libraries. If you don't re-index, morphological variants of any new query terms are not found, and new idioms are ranked lower than they should be ranked.

To delete the indexes and re-index an entire library, see *To delete the index files and re-index the library*: on page 202.

Setting up custom dictionaries

This section explains how to setup a user-defined dictionary for Get-Answers. A user-defined or custom dictionary is also called a search engine thesaurus. To setup a custom dictionary, you need to perform the following tasks.

- Step 1** Familiarize yourself with the following two files `expand.wgt` and `semantic.db`.
- Step 2** Set up the user dictionary folders.
- Step 3** Modify `expand.wgt`.
- Step 4** Modify `semantic.db`.
- Step 5** Set up the search engine to accept a query with idioms.
- Step 6** Create cross references and indexes for the new user dictionary.
- Step 7** Re-start the Get-Answers search engine and test it.

`expand.wgt` and `semantic.db`

When you begin setting up a custom dictionary, you should familiarize yourself with the files `expand.wgt` and `semantic.db`. The file `semantic.db` holds all of the word associations. The file `expand.wgt` holds the association rules for matching the words within `semantic.db`.

Setting up the user dictionary folders

You need to create a new blank user dictionary in order to create space for your custom dictionary.

To create a new blank user dictionary:

1. Locate the `rw_english` folder. By default this is located at `C:\getanswers\resource\rw_english`.
2. Create a subfolder for your user dictionary. Give the folder a custom name such as “userdict” with eight characters or less and without spaces.

- 3 Create the following empty text files within this folder. The easiest way to do this in Windows is to right-mouse click in your new user dictionary folder and select **New > Text Document**.
 - a Create a text file named `irreg.db`.
 - b Create a text file named `semantic.db`.
- 4 Copy the file `expand.wgt` from the standard dictionary folder into your new user dictionary folder. By default this is located at `C:\getanswers\resource\rw_english\dict\expand.wgt`.

To setup preferences to locate your new user dictionary:

- 1 Open the file `lang.cfg` in a text editor. By default this is located at `C:\getanswers\resource\rw_english\lang.cfg`.
- 2 Locate the line: `DICTIONARY = ".\dict";`
- 3 Add the following line directly after the line (`DICTIONARY = ".\dict";`)
`DICTIONARY = ".\userdict";`
- 4 Save and close the file `lang.cfg`.

Modifying `expand.wgt`

You need to modify the file `expand.wgt` to setup the rules for creating an exact match between two or more group's terms.

To modify `expand.wgt`:

- 1 Open the file `...\userdict\expand.wgt` in a text editor.
This shows a list of numbers and their search ranking rules.
- 2 Locate the last line in the file.
It should be something like this: `27 0.18 ;wn verb participle`.
- 3 Create a new line after the last line that looks like this: `28 1.00 ;force exact match`
The 28 is a new number we use to associate related terms
The 1.00 is the highest value we can use, and it associates terms as an exact match.
“`;force exact match`” is a comment.
- 4 In the first few lines of the `expand.wgt` file are the lines:
`;`the next line has the types which are index entry points to `semantic.db`

3 4 7 10

Add 28 to the end of the series of numbers so that the line becomes:

3 4 7 10 28

- 5 Save and close the file `expand.wgt`.

Modifying semantic.db

You need to modify `semantic.db` with a list of grouped terms that you want associated with one another. For this example all words you associate are considered exact matches. Searching for any word in the group will find all other words in the group. The exception to this are idioms (multi-word terms). It is OK to use idioms, but the changes used in this document will only associate the terms in one direction: single-word finds idiom, *not* idiom finds single-word. Idioms can exist in source documents, but it doesn't help to search with them.

To modify semantic.db:

- 1 Open the file `...\userdict\semantic.db` in a text editor.
- 2 Add your list of grouped terms to this document using the following guidelines:
 - a Your groups will contain a root term followed by all other related terms.
 - b Format your groups with the following syntax:
 - First Line: A period (.)
 - Second Line: The “at” symbol (@), followed by a single upper-case character denoting the part of speech (e.g., N).
 - Third line: The number 28 (denoting the root term), followed by a space, followed by the Root term in all upper-case. Any term greater than three words will not work. Limit your terms to one to three words.
 - Following lines: The number 28 (or as denoted set up in the previous for an “exact match”), followed by a space, followed by the associated term or idiom in all upper-case. Any term greater than three words will not work. Limit your terms to one to three words.
 - Last line/First Line of next group: A period(.)

For example:

```
.
@N
```

28 RETRIEVER
 28 MYDOGSPOT
 28 SPOT
 28 GOLDEN
 28 DOG
 28 GOLDEN RETRIEVER
 28 MY DOG SPOT
 .
 @N
 28 PERSIAN
 28 MYARISTOCAT
 28 ARISTOCAT
 28 EXPENSIVE
 28 CAT
 28 EXPENSIVE CAT
 28 MY ARISTOCAT
 .

3 Save and close the file `semantic.db`

Setting up the search engine

This section explains how to setup the search engine to accept a query with idioms (multi-word terms). Idioms are multi-word terms such as MY DOG SPOT or GOLDEN RETRIEVER, where you want the entire phrase to be treated as a single word. By default you can have idioms in your documents and find them, but you will not be able search using an idiom and find other related terms.

For example, using the sample terms above a search for MYDOGSPOT finds the idioms “GOLDEN RETRIEVER” and “MY DOG SPOT” if they exist in your source documents, but you cannot search for “MY DOG SPOT” and find MYDOGSPOT.

To search with idioms in your query string:

- 1 Backup ALL files and subfolders of the `rw_english` folder before performing this procedure.

By default these files are located at `c:\getanswers\resource\rw_english`.

- 2 Now that you've made a backup, open the file `rw_english.ilx` in a text editor.

By default this file is located at

`C:\getanswers4\resource\rw_english\rw_english.ilx`.

- 3 Insert each idiom into this alphabetical list in its exact alphabetized location using the following syntax:

IDIOM TERM in all caps, followed by a colon (:) followed by the letter denoting the part of speech, such as N.

Examples:

GOLDEN RETRIEVER:N

MY DOG SPOT:N

Warning: Failure to put ALL idioms in EXACT alphabetized order causes the search engine to fail with errors upon starting. If this happens you will see an error about the terms not being in alphabetical order. Fix the order and try again.

- 4 Save the file.
- 5 Re-index the main Get-Answers dictionary (not your user dictionary) using the following command:

```
C:\getanswers\bin>dict_xrf.exe
c:\getanswers\resource\rw_english\dict
```

Note: This is not the user dictionary “userdict.” This is the dictionary “dict” that ships with Get-Answers.

- 6 Restart the search engine.

Warning: Back up the file `rw_english.ilx` after making changes. This file may be removed or overwritten if you re-install or upgrade Get-Answers.

You should now be able to search with an idiom and find all other related terms. For example a search for MY DOG SPOT finds MYDOGSPOT.

Creating cross references and indexes

You can now create cross references and indexes for the new user dictionary.

To create cross references and indexes:

- 1 Open a DOS command prompt.
- 2 Change directory to the Get-Answers “bin” directory.
By default this is at `c:\getanswers\bin`.
- 3 At the command prompt, run the following command to index the dictionary located, for this example located at `c:\getanswers\resource\rw_english\userdict`:
`C:\getanswers\bin>dict_xrf.exe`
`c:\getanswers\resource\rw_english\userdict`
- 4 Press **Y** then **ENTER** at the following prompt:
This utility creates cross-references for the following files:
`semantic.db` and `irreg.db`.
Continuing deletes the files `semantic.xrf` and `irreg.xrf` in the following directory (a dot means current directory):
`c:\getanswers\resource\rw_english\userdict`
The files `morph.lex` and `idiom.lex` in the same directory are also deleted.
Do you wish to continue? [press **Y** then **ENTER** to continue]
- 5 You should get the following confirmation:
Processing.....
Finished.

Re-starting and testing the Get-Answers search engine

Because this is a query-only dictionary, you only need to restart the Search Engine Server when changes are made. If you are creating a new query+index dictionary then you need to re-index all your documents.

To restart the Search Engine Server:

- 1 Stop the Get-Answers Search Engine. To do this by default, select **Start > Programs > Get-AnswersSearchEngine4.1 > Stop Search Engine Server**.
- 2 Restart the Get-Answers Search Engine. To do this by default, select **Start > Programs > Get-AnswersSearchEngine4.1 > Start Search Engine Server**.
The query engine will now engage the new query-only dictionary when performs a search.

To test the Get-Answers search engine:

- 1 Add a document with a term in one of your groupings, for example, GOLDEN.
- 2 Force the indexer to update so you don't have to wait. To do this, select **Start > Programs > Get-AnswersSearchEngine4.1 > Index Updated Documents**.
- 3 Search for a related term from your group, for example, SPOT.
You should get a hit on your document.

Customizing edit-on Pro

Get-Answers provides users with a text editor, edit-on Pro, for adding content and documents to the system. This section describes the administration and customization tasks for edit-on Pro.

Browser Settings

In order to use edit-on Pro, your browser must be setup to support Java. The standard settings for most browsers are okay for edit-on Pro. The following is a guide for setting up the edit-on Pro recommended settings.

To set up Microsoft Internet Explorer with Microsoft Java VM:

- 1 Click **Tools > Internet Options...**
The Internet Options window opens.
- 2 Click the **Security** tab. The security level for the content zone from where you load edit-on Pro must at least be set to *Medium* (default setting for Internet zone).
Note: edit-on Pro will not work in *High* security level.
- 3 If you have to use **Custom Level...** settings, ensure in the Security Settings window that *Microsoft VM Java Permissions* is not set to *Disabled Java*. The default setting for *Medium Level* security is *High safety for Java Permissions*. edit-on Pro runs with this setting.
- 4 Also, in the Security Settings window check in the *Scripting* section that *Scripting of Java Applets* is enabled.

To set up Netscape Navigator 6.x, 7.x and Mozilla 1.x with Sun JRE 1.4.1:

- 1 Click **Edit > Preferences...**
The Preferences window opens.
- 2 On the Category menu in the Preferences window, click **Advanced**.
- 3 In the Advanced section ensure that *Enable Java* and *Enable JavaScript for Navigator* are checked.

Java security considerations

Java applets run in a sandbox mode. By default, applets have no access to system resources outside the directory/environment from which they were launched; however, a signed applet can access local system resources, as allowed by the local system's security policy. The Java Development Kit 1.2 provides security tools so that end users and system administrators can sign applets and applications. Thus, they may define their local security policy, by specifying in a policy file how much access to local system resources a signed applet or application can have.

Running edit-on Pro as a signed applet

The edit-on Pro applet archive has been signed with a Thawte digital certificate (a Verisign company), to bypass the Java applet sandbox. Signing an applet archive guarantees that the applet is from the certificate owner (RealObjects in this case), and that the archive is the original and has not been tampered with. A signed applet will have access to system resources, which enables Cut and Paste feature to the system clipboard. To run a signed edit-on Pro applet:

- 1 Run edit-on Pro using the signed applet archive (edit-on-pro-signed.cab / edit-on-pro-signed.jar).
- 2 A “Security Warning” notification dialog box in Microsoft Internet Explorer or “Java Security” dialog box in Netscape Navigator 4.7 or Netscape Navigator 6.x appears.
- 3 In:
 - Microsoft Internet Explorer 5.0:
To continue loading the edit-on Pro signed applet, click “Yes”. To abort loading, click “No”. The “Always trust content from RealObjects GmbH” option, should be checked if you want your browser to insert RealObjects in as a trusted publisher, therefore preventing it from displaying this dialog box again.
 - Netscape Navigator 4.7:
To continue loading the edit-on Pro signed applet, click “Grant”. To abort loading, click “Deny”. The “Remember this decision” option, should be checked if you want your browser to put RealObjects in as a granted vendor, therefore preventing it from displaying this dialog box again.
 - In Netscape Navigator 6.x:

To continue loading the edit-on Pro signed applet, click “Grant this session”. To abort loading, click “Deny”. The “Grant always” button, should be clicked if you want your browser to put RealObjects in as a granted vendor, thus preventing it from displaying this dialog box again.

Removing RealObjects from trusted publisher in Microsoft Internet Explorer 5.0

If RealObjects is registered as a trusted publisher for your browser, the “Security Warning” notification dialog box will not appear to warn you for the edit-on Pro signed applet.

To remove RealObjects from your browser’s list of trusted publishers and display this dialog box again:

- 1 In the browser, click **Tools > Internet Options ...**
 - 2 In the Internet Options dialog click the **Content** tab.
 - 3 Click the **Publishers...** button in the Certificates frame to list the trusted publishers in your browser.
 - 4 In the Authenticode™ Security Technology dialog box, select RealObjects GmbH from the Trusted Publisher list.
 - 5 Click **Remove** to remove it from the trusted publisher list for your browser.
- The Security Warning notification dialog box should appear every time you load edit-on Pro signed applet until you again register RealObjects as trusted publisher.

Removing RealObjects from Granted Vendors in Netscape Navigator 4.x:

- 1 In the browser window, click **Communicator > Security Info**.
- 2 In the Security Info dialog, select Java/JavaScript.
- 3 Select RealObjects GmbH from the list of vendors that are granted access.
- 4 Click **Remove**.

The Java Security notification dialog box should appear every time you load the edit-on Pro signed applet, until you add RealObjects to the trusted publishers again.

Removing RealObjects from Granted Vendors in Netscape Navigator 6.1:

- 1 In Netscape Navigator 6.1, Granted Vendors can be removed using the Java Plug In 1.3.1 Control Panel in Control Panel.
- 2 Click the **Certificates** tab.

- 3 Select “RealObjects GmbH” from the list of granted vendors.
- 4 Click **Remove**.

The Java Security notification dialog box should appear every time you load the edit-on Pro signed applet, until you add RealObjects to the trusted publishers again.

Style sheets support

This section describes how to set up and use the Style Properties dialog and Style Sheet Class Selector Choice menu available with edit-on Pro.

Style Properties dialog

You can use the Style Properties dialog to edit the style sheet. To display the icon which allows access to the style properties dialog in the toolbar, the appropriate definitions must be put in the `toolbar.xml` file. The following is an example of a corresponding fragment of the `toolbar.xml` file.

```
<toolbar>
...
  <icon paramname="PROPERTIESDIALOG"> />
</toolbar>
```

The Style Properties dialog provides an interface that allows the user to create, change, and delete styles. The styles listed in the Style Properties dialog are the editable styles.

Adding new styles

The styles can be added using two types of selectors:

- HTML tags

To add a new style to the document using the HTML tags selector:

- 1 Select the **HTML Tags** selector from the HTML Tags choice menu.

As you select the HTML tag, the name (selector) text field displays the corresponding selector. The new style will have the corresponding HTML tag as its selector, and it will be listed in the list on the left side of the dialog.
- 2 Click **New**.

example:

If you select *strong* from the HTML Tags Choice menu and click New, the new style will have *strong* as its selector.

Note: *Strong* defines a new style that can only be applied to the *strong* HTML Tag.

- Name (Selector)

To add a new style to the document using the name selector:

- 1 Type the selector in Name (Selector)
- 2 Click New.

When something is typed in Name (Selector), the HTML Tag choice menu is emptied. The new style has the corresponding name selector and is listed on the left side of the dialog.

To create a new style, you should specify the properties of the style you want to create. For more information on how to create properties of the style, see *Modifying styles* on page 216.

example:

If you type *.class1 from the HTML Tags choice menu, the new style will have *.class1 as its selector.

*.class1 defines a new style that can be applied to any HTML tag that has the class=class1 attribute.

Note: Adding a new style will not take effect if none of the style properties are specified. You should specify at least one property for the new style to take effect.

Modifying styles

Styles can be modified by altering their properties. The style properties dialog allows for the following types of style modifications:

- Style properties

Style properties allow the user to modify simple properties of the style. These include:

- font type
- font size
- bold
- italic

- underline
- font color
- background color

- **Advanced style properties**

Advanced style properties are properties not present in the style selector. The variation of properties which can be modified is virtually limitless, but edit-on Pro supports only a fragment of the available style sheet definitions. You can add name-value pair attributes using the Add button in the Advanced Style Properties. You can also modify and remove existing advanced style properties.

To add name-value pairs:

- 1 Click **Add** in the Advanced Style Properties window.

A dialog opens which requests the name-value pair of the style's attribute.
- 2 Type the name-value pair in the text field.
- 3 Click **OK**.

The name-value pair is inserted into the Advanced Styles Properties list.

To modify an existing advanced style property:

- 1 Select the style from the style properties list
- 2 Click **Modify**.

A dialog opens that allows you to make the appropriate modifications.
- 3 Click **OK**.

The modified name-value pair is inserted into the Advanced Styles Properties list.

To remove an existing advanced style property:

- 1 Select the style from the style properties list
- 2 Click **Remove**.

Changing a style's name

You can use the Properties window to change a style's name.

To change a style's name:

- 1 Select the style from the list of styles.

- 2 Type the new name in Name (Selector) or select an item from HTML Tags choice menu.
- 3 Click **Change Name**.

Deleting a style

You can use the Properties window to delete a style.

To delete a style:

- 1 Select the style from the list of styles.
- 2 Click **Delete**.

Style sheet class selector choice menu

The style sheet can be applied to the HTML tag in the current cursor position using the Style Sheet Class Selector choice menu. To display the menu on the toolbar, the appropriate definitions must be put in the `toolbar.xml` file. The following is an example of a fragment of the `toolbar.xml` file.

```
<toolbar>
...
<choice paramname="STYLESHEET" />
...
</toolbar>
```

The `STYLESHEET` parameter allows the user to select stylesheet classes, which can then be applied into a selection of text using a drop-down list box. This feature is disabled when there is no selection. The Style Sheet Class Selector Choice Menu is context sensitive, meaning that the classes listed in the choice menu will change in relation to the HTML tags in the cursor position.

Insert span

The style sheet can be applied to the HTML tag in the current cursor position, when there is a selection using the 'Insert Span' button. To display the insert span icon in the toolbar, the appropriate definitions must be put in the `toolbar.xml` file. Following is an example of a fragment of the `toolbar.xml` file.

```
<toolbar>
...
<icon paramname="INSERTSPAN" />
```

```
...
</toolbar>
```

The INSERTSPAN parameter creates an icon that when clicked asks for the stylesheet class to apply to the span. The available classes are generic and span context classes. After pressing OK, a span tag pair is inserted. The user may use this feature, to insert a span tag around a selection of text, and to apply a style sheet class into that tag. Please note that the classes listed in the class choice menu of the Insert Span dialog are the styles which have generic selectors (e.g., *.class1) and/or the styles that have span selectors (e.g., span.class1).

Displaying unknown tags

Unknown tags will be preserved and displayed as yellow marks within the WYSIWYG View, if the toolbar button is activated. An “unknown tag property” dialog opens when clicking the right mouse button on the yellow marks. The contents of the unknown tag can be edited and changes are preserved.

Online help in edit-on Pro

To make the online help accessible from the help button on the toolbar, please make sure that the following settings are done:

- The HELP API parameter is set to specify the URL of the help file in HTML format. The help will be displayed in a new browser window when the user clicks on the HELP icon.
- The HELP icon must be activated by setting the HELP parameter in the toolbar definition file.

The Online Help can be found in the “eophelp” subdirectory of the edit-on Pro main installation directory (usually “eopro”). It is available in US English, Spanish, French, and German.

Customizing the edit-on Pro spelling checker

You can customize the spelling checker used in the edit-on Pro authoring tool.

To customize the spelling checker:

- 1 Add the spelling checker library to the HTML Applet tag:


```
<APPLET code="EditorApplet.class" archive="edit-on-pro.jar,ssce.jar"
name=MyEditor>
  <PARAM name="CODEBASE" value="http://www.yourcategory.com/eopro/">
  <PARAM name="CABBASE" value="edit-on-pro.cab,ssce.cab">
  .
  .
  .
</APPLET>
```
- 2 Add the parameter SPELLCHECKPROPERTIES to the HTML Applet tag to specify the URL address of the spelling checker properties file relative to the applet code base. The spelling checker properties file defines which options to set and which dictionaries/lexicons to open. Change the parameter value to change the dictionary/lexicon.


```
<PARAM name="SPELLCHECKPROPERTIES" value="sc - americanenglish.txt">
```
- 3 Add the parameter SPELLCHECK in the button ordering file to make the spelling checker icon visible.
- 4 Copy the dictionary/lexicon files specified in the spelling checker properties file to the proper location on the web server.

Spelling checker properties

A settings in the spelling checker properties file can be modified. The settings including keys and options.

MainLexicon and UserLexicon

The spelling checker opens main lexicons using keys named MainLexicon, where n is a number ranging from 1 to 99. The first main lexicon must be specified by MainLexicon1, and any other main lexicons must be numbered sequentially starting with MainLexicon2. The lexicon stops if the MainLexicon sequence numbers break.

UserLexicon and MainLexicon property settings have the following form:

```
{Main|User}Lexiconn=name [, access method] [, format]
```

n: Sequence number of the main or user lexicon, ranging from 1 to 99. Lexicons open in the specified sequence.

name: Name of the lexicon file, resource, or URL (depending on the access method).

access method: Method used to access the named lexicon:

- file: The lexicon is opened as a local disk file (default).
- resource: The lexicon is opened as a resource using `java.lang.Class.getResourceAsStream` method.
- url: The lexicon is opened as a URL using `java.net.URL`'s `openStream` method.

format: The format of the lexicon. The format defaults to "t" unless the extension part of the name parameter is "clx" or "uclx," in which case the default format is "c." "t" represents a text lexicon. "c" represents a compressed lexicon.

The spelling checker accesses the lexicon files relative to the code base. The lexicon files can reside in the same directory as the applet or in a subdirectory.

Currently available MainLexicons include:

- American English MainLexicon
- British English MainLexicon
- Canadian English MainLexicon
- German MainLexicon
- French MainLexicon
- Spanish MainLexicon
- Finnish MainLexicon
- Dutch MainLexicon
- Swedish MainLexicon
- Italian MainLexicon
- Norwegian
- Danish
- Brazilian

- American Medical
- British Medical

A custom Lexicon can be created by making a new text lexicon file or by altering an old one. The text lexicon is a mere text file which can be edited using any text file editor (e.g. < Notepad). Custom words can be added by simply appending the word at the end of the word list, inside the text lexicon file. The “ADDSPELLCHECKWORDURL” tag in the configuration file can be used to specify the CGI/ASP/PHP/JSP URL, which appends the new word to the related text lexicon file.

Spelling checker options

You can make the option value “true” or “false.” The option is set if the value is “true.” The option’s default value is used if the corresponding key is not included in the Properties.

The options affect the way the spelling checker operates. In most cases, options are enabled by setting their values to true and disabled by setting their values to false.

- ALLOW_ACCENTED_CAPS_OPT: If set to true, capital letters containing accents are considered acceptable. If set to false, words containing accented capitals are considered misspelled. Setting this option to false degrades performance. Default: true.
- CASE_SENSITIVE_OPT: Set to true if words with different letter-case patterns should be treated as different words. Set to false if words containing different case patterns should be treated as identical. Setting this option to false degrades performance. Example: If set to true, treat *Canada* and *canada* as two different words; if set to false, treat *Canada* and *canada* as the same word. Default: true.
- IGNORE_CAPPED_WORD_OPT: Set to true if words should be ignored (skipped) if they begin with an uppercase letter. Set to false if the words should be checked for spelling errors. Example: If set to true, ignore *Clarkson*; if set to false, check *Clarkson*. Default: false.
- IGNORE_ALL_CAPS_WORD_OPT: Set to true if words consisting entirely of uppercase letters should be ignored (skipped). Set to false if the words should be checked for spelling errors. Example: If set to true, ignore *ASAP*; if set to false, check *ASAP*. Default: false.

- **IGNORE_category_NAMES_OPT**: Set to true if words that appear to be Internet category names should be ignored (skipped). Set to false if the words should be checked for spelling errors. Words are considered to be Internet category names if they contain at least one “dot” (.) and at least two alpha-numeric characters in a row. Example: If set to true, ignore *wintertree-software.com*; if set to false, check *wintertree-software.com*. Default: false.
- **IGNORE_MIXED_CASE_OPT**: Set to true if words containing an unusual mixture of uppercase and lowercase letters should be ignored (skipped). Set to false if such words should be checked for spelling errors. Example: If set to true, ignore *PrintScreen*; if set to false, check *PrintScreen*. Default: false.
- **IGNORE_MIXED_DIGITS_OPT**: Set to true if words containing a mixture of letters and digits should be ignored (skipped). Set to false if such words should be checked for spelling errors. Example: If set to true, ignore *Win95*; if set to false, check *Win95*. Default: false.
- **IGNORE_NON_ALPHA_WORD_OPT**: Set to true if words that contain no alphabetic characters should be ignored (skipped). Set to false if the words should be checked for spelling errors. Example: If set to true, ignore *12345*; if set to false, check *12345*. Default: true.
- **REPORT_UNCAPPED_OPT**: Set to true if uncapitalized words which exist in the lexicons in capitalized form only should be reported (via **UNCAPPED_WORD_RSLT**). Set to false if uncapitalized words should not be reported. Example: If set to true, report *canada*; if set to false, do not report *canada*. Default: true.
- **REPORT_MIXED_CASE_OPT**: Set to true if words containing an unusual combination of upper and lowercase letters should be reported (via **MIXED_CASE_WORD_RSLT**). Set to false if such words should not be reported. Example: If set to true, report *Tuesday*; if set to false, do not report *Tuesday*. Default: false.
- **REPORT_MIXED_DIGITS_OPT**: Set to true if words containing a combination of letters and digits should be reported (via **MIXED_DIGITS_WORD_RSLT**). Set to false if such words should not be reported. Example: If set to true, report *June5*; if set to false, do not report *June5*. Default: false.
- **REPORT_DOUBLED_WORD_OPT**: Set to true if two occurrences of the same word in a row should be reported (via **DOUBLED_WORD_RSLT**). Set to false if doubled words should not be reported. Example: If set to true, report *the the*; if set to false; do not report *the the*. Default: false.

- **SPLIT_HYPHENATED_WORDS_OPT**: Set to true if hyphens (-) should be treated as word separators, and each subword checked individually. This word splitting is done only if the hyphenated form of the word does not exist in any open lexicon. The word is considered correctly spelled if all subwords are correctly spelled. Set to false if hyphenated words should be checked in their entirety. Example: If set to true, and *bright-blue* was not found in the open lexicons, check both *bright* and *blue* and treat *bright-blue* as correctly spelled if both words are found; if set to false, report *bright-blue* as misspelled if not found in the open lexicons. Default: true.
- **SPLIT_CONTRACTED_WORDS_OPT**: Set to true if apostrophes should be treated as word separators, and each subword checked individually. This word splitting is done only if the contracted form of the word does not exist in any open lexicon. The word is correctly spelled if all subwords are correctly spelled. Default: false.
- **SPLIT_WORDS_OPT**: Set to true if words should be treated as a series of concatenated subwords, and each subword checked individually. This word splitting is done only if the original word is not found in any open lexicon. The word is correctly spelled if all subwords containing two or more characters are correctly spelled. Default: false.
- **STRIP_POSSESSIVES_OPT**: Set to true if possessives of the form 's and s' should be removed from words before checking their spelling. The main lexicons included with the Sentry SDKs contain no possessive word forms, so this option should be enabled when using these lexicons. Set to false if words should be checked with their possessives intact. Default: true.
- **SUGGEST_SPLIT_WORDS_OPT**: Set to true if the suggest method should attempt to split words into two valid subwords. Set to false if split words should not be suggested. Example: If set to true, suggest *the boy* as a replacement for *theboy*; if set to false, do not suggest *the boy*. Default: false.

Example properties file

The following list shows the default settings for American English. This file is the `sc-americanenglish.txt` file in the `eopro` folder of the base server path to `oaa`.

```
#Settings for American English dictionary
UserLexicon1=lex/userdic.tlx,url,t
UserLexicon2=lex/correct.tlx,url,t
UserLexicon3=lex/accent.tlx,url,t
```



```

MainLexicon1=lex/ssceam.tlx,url,t
MainLexicon2=lex/ssceam2.clx,url,c
REPORT_UNCAPPED_OPT=true
IGNORE_CAPPED_WORD_OPT=false
SPLIT_WORDS_OPT=false
IGNORE_NON_ALPHA_WORD_OPT=true
REPORT_MIXED_CASE_OPT=false
REPORT_DOUBLED_WORD_OPT=true
IGNORE_ALL_CAPS_WORD_OPT=false
ALLOW_ACCENTED_CAPS_OPT=true
MinSuggestDepth=50
SPLIT_HYPHENATED_WORDS_OPT=true
Suggestions=typographical
IGNORE_MIXED_CASE_OPT=false
STRIP_POSSESSIVES_OPT=true
REPORT_MIXED_DIGITS_OPT=false
SUGGEST_SPLIT_WORDS_OPT=true
IGNORE_DOMAIN_NAMES_OPT=true
IGNORE_MIXED_DIGITS_OPT=false
SPLIT_CONTRACTED_WORDS_OPT=false
Comparator=Typographical
CASE_SENSITIVE_OPT=true

```

Adding words to the spelling checker

You can configure edit-on Pro so that users can add words to the spelling checker.

To activate the Add Word to spelling checker feature in edit-on Pro:

- 1 Set the ADDSPELLCHECKWORDURL parameter in the configuration file.

Example:

```

...
<spellingcheckers>
...
<addspellcheckwordurl url="http://www.yourdomain.com/eopro/AddWord.jsp"
/>
...
</spellingcheckers>
...

```

- 2 Set the url attribute to the URL address where the Server-side script (CGI/ASP/PHP/JSP file) is available.

The CGI/ASP/PHP/JSP script is responsible for appending the new word to the corresponding text lexicon file.

The following listing shows a sample of a JSP script that adds words to the corresponding lexicon file:

```
<%@ page import="java.io.*" %>
<html>
<head>
<title>Add Word</title>
</head>
<body>
<%
    String language = request.getParameter("LANG");

    String strFile = "D:\\dictionary-directory\\" ;
    if (language.equalsIgnoreCase("US English"))
        strFile = strFile + "userdicam.tlx";
    else if (language.equalsIgnoreCase("German"))
        strFile = strFile + "userdicge.tlx";

    File fileDict = new File (strFile);
    RandomAccessFile dict = new RandomAccessFile(fileDict, "rw");

    boolean line = true;
    String strAdded = " ";
    strAdded="\r\n"+request.getParameter("WORD");
    while (line){

        String s = dict.readLine() ;
        if (s == null){

            dict.writeBytes(strAdded);
            break;

        }
    }
    dict.close();
%>
</body>
</html>
```

Note: The Variable LANG contains the spell checker's active language, and the variable WORD contains the new word to add to the dictionary.

When the user presses the **Add Word** button in the Spelling Checker dialog:

- edit-on Pro passes the value of the variables LANG and WORD to the server-side script (CGI/ASP/PHP/JSP file) as a POST request.

- The server-side script adds the value of variable WORD into the lexicon file specified by the variable LANG.
- edit-on Pro loads the new lexicon file (dictionary) with the new word the next time the spelling checker action is invoked.

10 Get-Answers Workflows

CHAPTER

Workflow is a tool you can use to route documents through the review process automatically. Workflow consists of business processes, which are objectives for your work. For example, reviewing a document is a business process. Business processes contain activities. Each activity forwards the goal of the business process. The activity “publish document” is the end result of the review process.

Note: Workflow is a tool that professional services customizes. The only way to customize the out-of-the-box Get-Answers workflows is to add an additional and identical Editor or Reviewer activity before the final Owner activity. It cannot be customized otherwise without professional services.

This chapter describes how to use workflow in general and includes the following topics:

- *Defining workflow templates* on page 230
- *Using Workflow Administration* on page 260
- *Using the Request List* on page 282

Defining workflow templates

The workflow templates are process definitions for business processes associated with a business object, such as contracts or projects. Business objects can be attached to a specified workflow template designed for processing work for the business object.

The Glossary of this book includes definitions of workflow terms.

This section includes explanations for:

- *Creating a workflow template* on page 230
- *Creating a workflow template from another template* on page 253
- *Modifying a Workflow template* on page 253
- *Deleting a Workflow template* on page 255
- *Creating a Component template* on page 257

To create an workflow template:

- Step 1** Identify a process type: standalone, business object, embedded data
- Step 2** Create activities for the process workflow: task, approval, message, script, subprocess.
- Step 3** Create Select activities for the process workflow: branches in the workflow.
- Step 4** Create Jump activities for the process workflow.
- Step 5** Add component templates to the process workflow.
- Step 6** Modify an activity in the process workflow as required.

Creating a workflow template

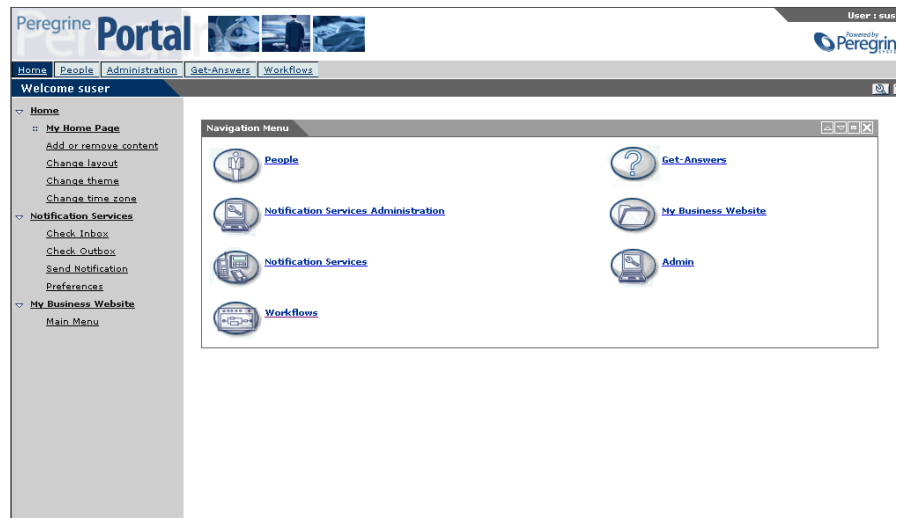
Workflow provides a graphical workflow designer for designing and creating workflow templates. After a workflow template is created and attached to a business process, process instances of the workflow template can be started.

Each process instance is routed according to the activities specified in the workflow template, but the workflow definition for a process instance is no longer linked to the workflow template. If changes to the routing are required during processing, the user can modify the workflow through the workflow designer for that specific process instance. The workflow template is not changed and future process instances are routed according to the workflow template.

Note: Capability (permission) must be assigned to a user before the user can modify a workflow route. Refer to the Chapter 4 for information about security and assigning capabilities.

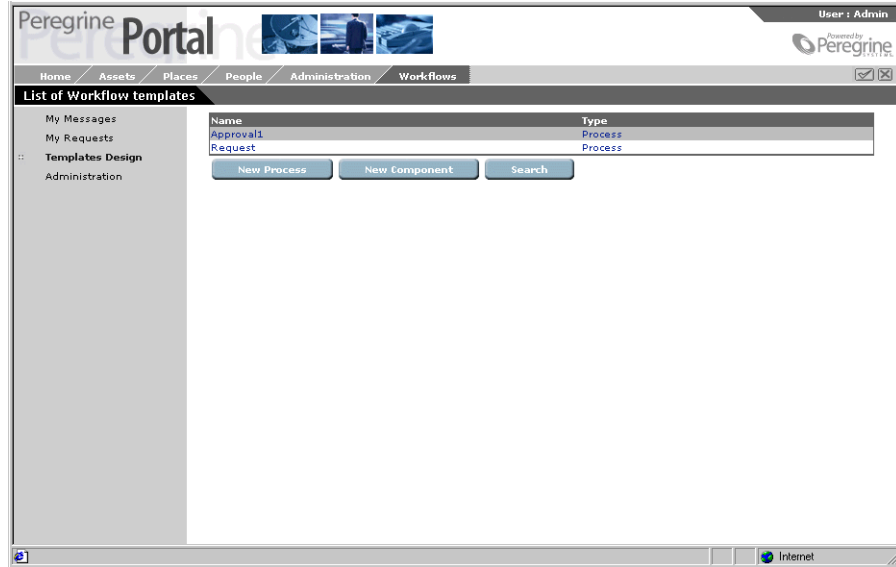
To create a workflow template:

- 1 Log on to your Web application to display the Navigation Menu on your Home page.



- 2 Click the Workflows tab or click Workflows from the Navigation Menu. The Workflow link appears in the left pane.

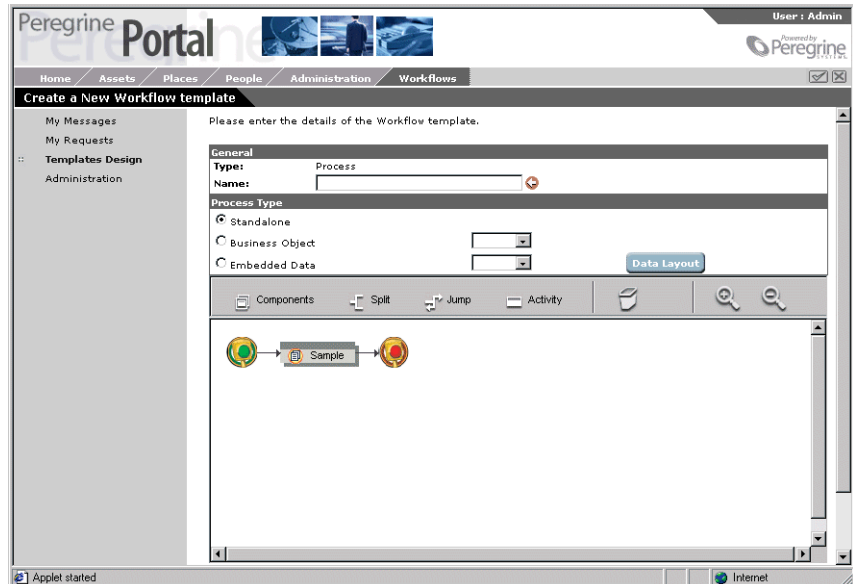
- 3 Click the **Templates Design** link to display the **List of Workflow templates** page.



Note: After workflow templates are defined, the template name and type (Process or Component), for each template appears in the list.

- 4 Click **New Process**.

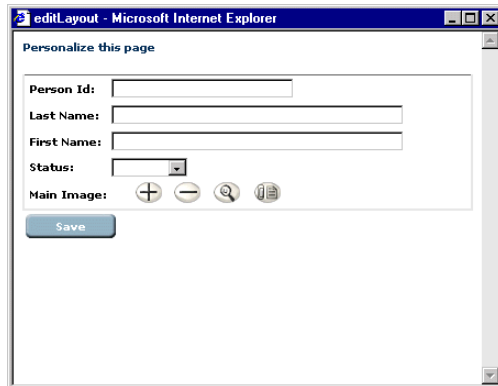
The Create a New Workflow template page appears.



The Type of Process entry is created by the system based on your selection of the **New Process** button.

- 5 In the **Name** text box, type the name of the new workflow template.
- 6 In the **Process Type** section, select one of the option buttons to define the process type associated with this workflow template.
 - **Standalone**—When the **Standalone** option button is selected, there is no link to a business object or to data.
 - **Business Object**—When you select the **Business Object** option button, the workflow relates to a business object associated with your Web application.
 - **Embedded Data**—When you select the **Embedded Data** option button, the workflow relates to data. This data is not stored in the database, but is carried with the process.
- 7 If you selected the **Business Object** option button, select the business object from the associated drop-down list.
- 8 If you selected the **Embedded Data** option button:
 - a Select the entity or schema from the associated drop-down list.

- b Click **Data Layout** to display the **EditLayout** window.





You can change the data layout using the **Personalize this page** option at the top of the page. Refer to your Web application documentation for information on the Personalization feature.




- c Click **Save** to exit the EditLayout window and return to the **Create a New Workflow** page.

The workflow template defines a specific process definition. The name assigned to the template *must* be unique and should reflect the process definition.



Each workflow template must have a Start and End activity. When initially displayed, the workflow designer contains the Start and End activity, and includes a sample activity that can be modified for use in your workflow template or can be deleted. See *Modifying an activity* on page 251 and *Deleting an activity* on page 252.

- 9 In the workflow designer, create and add activities to the workflow template using the toolbar icons described in the following table.

Icon	Description
	Select a component from the template list. See <i>To add a component template</i> : on page 250 for information on adding an activity from the template list.
	Create a new Select activity. See <i>To create and add a Select activity</i> : on page 245 for information on adding a Select activity.

Icon	Description
	Create a new Jump activity. See <i>To create and add a Jump activity</i> : on page 248 for information on adding a Jump activity.
	Create a new activity. See <i>To create and add a new activity</i> : on page 235 for information on adding a new activity.
	Trash. See <i>To delete an activity</i> : on page 252 for information on deleting an activity from a workflow template.


In addition to the activity icons on the toolbar, zoom functionality is provided by the following toolbar icons.

Icon	Description
	To zoom in on the workflow template graphic, click the Zoom in icon until the required magnification is achieved.
	To zoom out on the workflow template graphic, click the Zoom out icon.

Creating a new activity

These activities represent the basic activities used when defining a workflow template for a specific process definition. An activity can be one of four types: Task, Approval, Message, or Script.

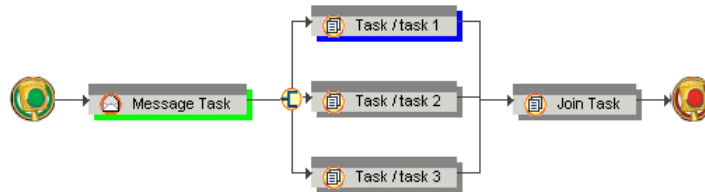
To create and add a new activity:

-  Position the cursor over the Activity icon, then click and hold down the left mouse button.
- Drag the Activity icon over an activity so that the new activity precedes, follows, or is parallel to that activity.
Notice that a rectangle outlined in red appears along with the icon.
- To select the placement of the new activity, position the red rectangle in one of the positions described in the following table and release the left mouse button.

Note: The position of the new activity is determined by where the red rectangle is located when you release the mouse button.

When positioned...	The activity is placed...
over the first half of the current activity	before the current activity
over the last half of the current activity	after the current activity
over the top half of the current activity	above the current activity
over the bottom half of the current activity	below the current activity

Parallel routing is defined by creating activities above or below a current activity (AND-Split). The activities are then joined later in the process by adding an activity after the parallel activities (AND-Join).



After you click the mouse button, the **Workflow** window opens. You define the details for the new activity through this window.

- 4 In the **Title** text box, type the title you want to display on the activity in the workflow designer.
- 5 Select the task type from the **Type** drop-down list.

Values for **Type** are:

- **Task**—a manual task
 - **Approval**—a task requesting approval
 - **Message**—an informational message that does not require user work
 - **Script**—a task performed by the system
 - **Subprocess**—another workflow process to be part of this workflow
- 6 In the **Subject** text box, type a short description of the task.
This description appears in the Screen Tip when the cursor is placed over the activity.
 - 7 In the **Description** box, type a full description of the task, or type the detailed message when the selected **Type** option button is **Message**.

- 8 For business objects type workflows, if you want to a customized form to display, select the name of the form from the **Form Name** drop-down list. Instead of the standard **Task Details** page, the selected form appears when viewing task details.
- 9 Click **Next**.

The Workflow window displays additional activity details. The activity details are different depending on the **Type** option button selected. If the select type is:

- Task or Approval, see *To complete the activity details for Task or Approval tasks*: on page 238.
- Message, see *To complete the activity details for a Message task*: on page 241.
- Script, see *To complete the activity details for a Script task*: on page 243.

To complete the activity details for Task or Approval tasks:

When the activity type is Task or Approval, the Workflow window shown below opens.

- 1 In the **Choose whom to notify to accomplish the task** section, select one of the option buttons to determine who is notified of the task.
 - User that initiated the process—The user who initiated the process is notified.
 - Supervisor of the User that initiated the process - Supervisor of User as indicated in the People module.

- By Person—The specific person selected is notified.
 - By Role—All users assigned to the selected role are notified.
 - By Script— A script determines one or more users to be notified.
- 2 If you selected the **By Person** option button:
 - a Click the search icon to display the Employee Lookup window.
 - b In this window, select the person you want to notify.
The name of the person selected appears next to the option button.
 - 3 If you selected the **By Role** option button, select the role from the associated drop-down list.
 - 4 If you want to notify the user, select the **User Notification** check box.
Note: The user are notified by the method indicated in the Notification Services tab. For information on Notification Services, refer to the *Notification Services* Documentation. When a user receives a notification, it contains standard message text and a link to the application to the associated activity.
 - 5 If you do not want to use the standard template, select the **Use custom template(s) for notification/reminder** check box.
 - 6 Click **Next**.

Workflow Activity details:

How many hours will this task require ?

Estimated time:

Calculate deadline by assignee work hours

Auto complete upon deadline

Auto complete default status: Time out ▼

Alarm

Type: None ▼

Skip below if alarm type is "None":

Time limit:

Send reminder to assignee

Send reminder to other user:

Update Go Back

- 7 In the **How many hours will this task require?** section, you have the following options:
 - a When the task is time-sensitive, type the number of hours allocated for the task to be completed in the **Estimated time** text box.

- b Select the **Calculate deadline by assignee work hours** check box if you want the deadline to be calculated according to the actual work schedule of the assignee as indicated in Notification Services. Doing so prevents the deadline from occurring on a day that the assignee normally has off.
- c Select the **Auto complete upon deadline** check box to cause the activity to go to completed state when the deadline is reached. If you select this option, also choose a default status from the drop-down list in the **Auto complete default status** field.

You can set an alarm for a time-sensitive task.

- 8 Select the alarm type from the **Type** drop-down list.

Values are:

- **None**—an alarm is not defined for the task.
- **Time elapsed since start of task**—alarm sent when the elapsed time (specified in **Time limit**) from the start of the task is reached.
- **Time before end of task**—alarm sent when the number of hours (specified in **Time limit**) prior to the end of the task is reached.

Note: When the alarm type is **Time before end of task**, the **Estimated time** text box must contain an entry for the number of hours allocated for the task.

- 9 Select the **Send reminder to assignee** check box to send the notification to the person assigned to the task.
- 10 Select the **Send reminder to other user** check box when you also want to send the e-mail notification to another person.

This person may be a supervisor or project manager who needs to know that a time-sensitive task is pending.

- 11 Click the search icon to display the Employee Lookup window.
- 12 Using the window, select the other user to notify.
- 13 Click **Update** to complete the task definition and display the activity in the workflow designer.

To complete the activity details for a Message task:

When the activity type is Message, the Workflow window shown below opens.

Workflow Activity details:

- 1 In the **Choose whom to notify to accomplish the task** section, select one of the option buttons to determine who is notified of the task.
 - User that initiated the process—The user who initiated the process is notified.
 - Supervisor of the User that initiated the process - Supervisor of User as indicated in the People module.
 - By Person—The specific person selected is notified.
 - By Role—All users assigned to the selected role is notified.
 - By Script— A script determines one or more users to be notified.
- 2 If you selected **By Person**, click the search icon to display the Employee Lookup window and select the person you want to notify
- 3 If you selected **By Role**, select the role from the associated drop-down list.
- 4 If you want to notify the user, select **Notify assignee of this task**.

Note: The user is notified by the method set in the Notification Services tab. For information on Notification Services, refer to the *Notification Services* documentation.

When a user receives a notification, it contains standard message text and a link to the application for the associated activity.

- a If you have defined a custom template in Notification Services, click the binoculars icon next to **Custom Message Template**. A window opens, for you to select the template you want to use.
 - b If you select a custom template that uses fields other than the default workflow fields, enter the name of the Java class used to render the custom template in the **Custom Render Class** field.
- 5 Click **Update** to complete the task definition and display the Message activity in the workflow designer.

To complete the activity details for a Subprocess:

When the activity type is Subprocess, the Workflow window shown below opens.

The screenshot shows a web browser window titled "editSubProcess - Microsoft Internet Explorer". The main content area is titled "Workflow Activity details for sub-process:". It contains several sections:

- Sub-process Template (required)**: A section with a label "OAA Workflow Template:" and a dropdown menu. To the right of the dropdown are two icons: a binoculars icon and a document icon.
- Use the following fields in the business object to start this sub-process**: A section with the instruction "Start subprocess using this datetime field:" followed by a text input field. Below this are four more text input fields labeled "Requester Id Field:", "Description Field:", "Business Object (Document):", and "Business Object Id Field:".
- Sub-process completion criteria**: A section with a checkbox and the text "Wait for completion of sub-process to go to the next step".
- Run a pre-process script**: A section with a label "Script Function Name:" and a dropdown menu. To the right of the dropdown are two icons: a binoculars icon and a document icon.

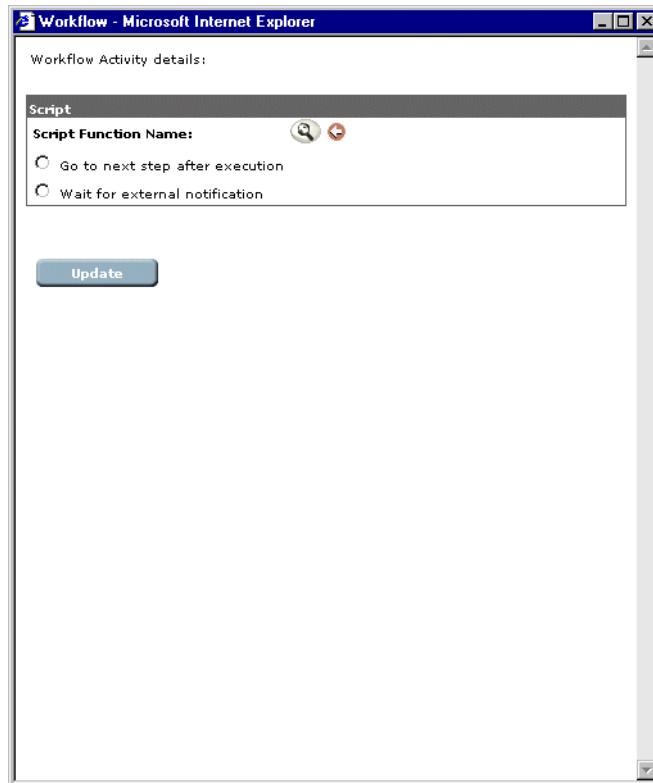
At the bottom of the form are two buttons: "Update" and "Go Back".

- 1 Use the drop-down list to select the OAA Workflow Template that is the subprocess.
- 2 If the subprocess relies a Business Object, populate the fields in the second section of the form.

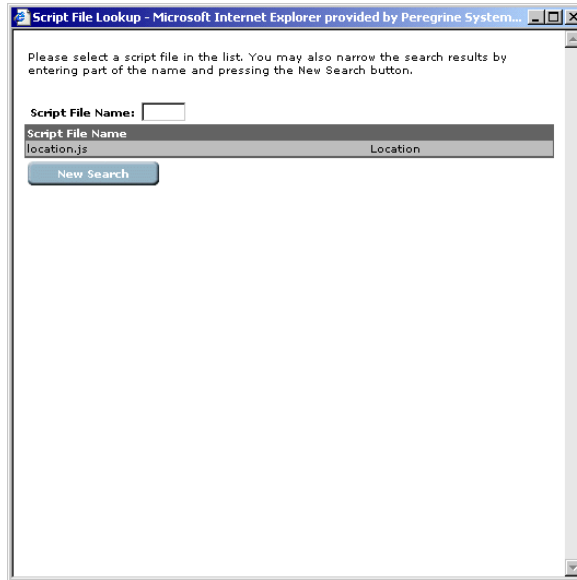
- 3 If the subprocess requires a status of complete prior to going to the next step the process, select the **Wait for completion of sub-process to go to the next step** check box.
- 4 If a script should run before the subprocess starts, use the drop-down list to select a **Script Function Name**.

To complete the activity details for a Script task:

When the activity type is Script, the Workflow window shown below opens.



- 1 Click the **binoculars** next to **Script Function Name** to display the Script File Lookup window.



- 2 Using this window and following the lookup instructions, locate and select the script function.

The selected script function name appears next to **Script Function Name** in the Workflow window.

- 3 Select one of the following option buttons to determine how the workflow process continues after the script is executes:

Go to next step after execution—Select this option button if you want the system to continue the workflow process after the script is executed.

Wait for external notification—Select this option button if you want the system to wait for an event from an external system before continuing the workflow process.

- 4 Click **Update** to complete the task definition and display the activity in the workflow designer.

Creating a Select activity

A Select activity is used to branch workflow routing (OR-Split). The workflow route is determined by a decision made in the previous activity or, in the case of a Custom Select, by the value returned after a script executes.

Note: If a Select activity, where the selection type is Approval, is present in the workflow, an Approval type activity must directly precede the Select activity.

To create and add a Select activity:



- 1 Position the cursor over the Split icon, then click and hold down the left mouse button.
- 2 Drag the Split icon over an activity so that the new activity precedes, follows, or is parallel to that activity.

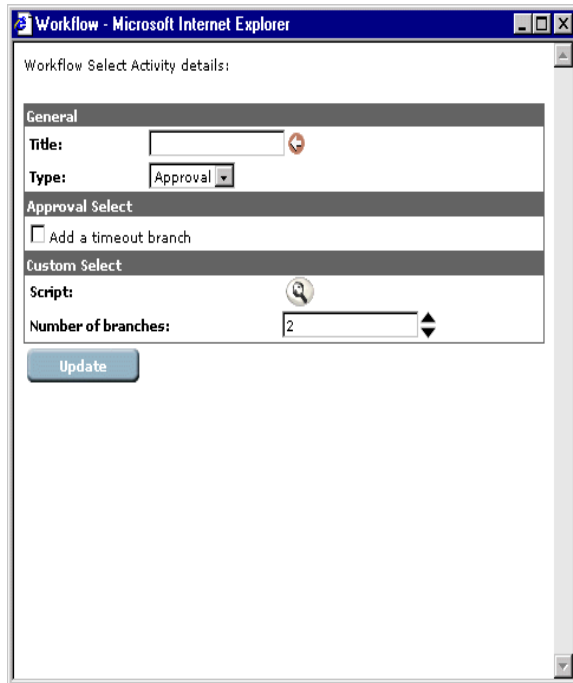
Notice that a rectangle outlined in red appears along with the icon.

- 3 To select the placement of the Select activity, position the red rectangle in one of the positions described in the following table and release the left mouse button.

Note: The position of the activity is determined by where the red rectangle is located when you release the mouse button.

When positioned...	The activity placed...
over the first half of the current activity	before the current activity
over the last half of the current activity	after the current activity
over the top half of the current activity	above the current activity
over the bottom half of the current activity	below the current activity

After you release the mouse button, the Workflow window opens.



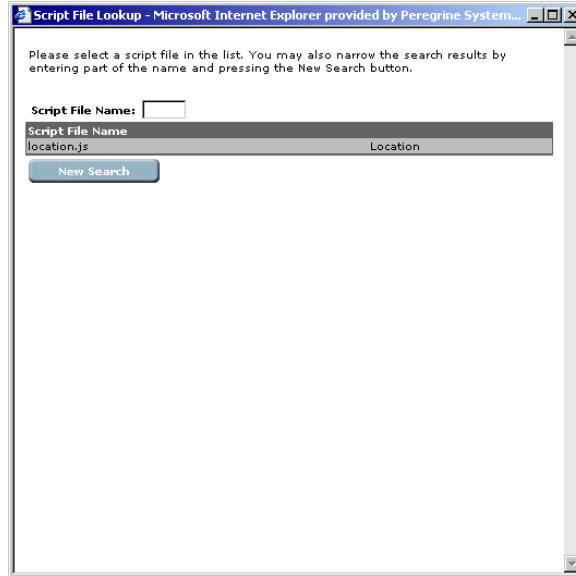
The screenshot shows a web browser window titled "Workflow - Microsoft Internet Explorer". The main content area is titled "Workflow Select Activity details:" and contains several sections:

- General**: A "Title:" text box with a red arrow icon to its right, and a "Type:" drop-down menu currently set to "Approval".
- Approval Select**: A checkbox labeled "Add a timeout branch" which is currently unchecked.
- Custom Select**: A "Script:" text box with a magnifying glass icon to its right, and a "Number of branches:" spin box currently set to "2".

At the bottom of the form is a blue "Update" button.

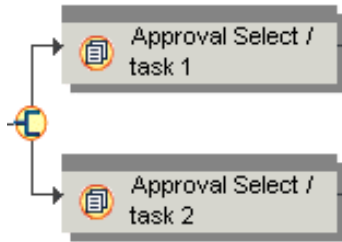
- 4 Type a name for the task in the **Title** text box.
The title appears (followed by the task number) on each of the activities associated with this activity.
- 5 Select the type of selection from the **Type** drop-down list.
Values are:
 - **Approval**—checks the previous activity to determine the routing requirements.
If you select this option and you have defined Time Out as the Auto Complete Default Status for the task, select **Add a time out branch** in the Approval Select section.
 - **Custom**—determines the routing requirements from the value returned by a script.If you selected Approval, go to step 8 to complete the procedure.

- 6 If you selected Custom, click the **binoculars** icon next to Script to display the Script File Lookup window.



- 7 Using this window and following the lookup instructions, locate and select the script function.
The selected script function name appears next to **Script** in the Workflow window.
- 8 Type or select the number of branches in the **Number of branches** text box.
- 9 Look at the task preceding this selection. If it meets all of the following criteria, you must select the **Add a time-out branch checkbox**.
 - **Auto complete upon deadline** is activated
 - **Auto complete default status** is Time Out.
- 10 Click **Update** to complete the Select activity definition and display the activity in the workflow designer.

A Select activity creates activities for each of the branches created.



The top activity (task 1) executes when the prior task is approved. The bottom activity (task 2) executes when the prior task is declined.

- 11 Click each of the branch activities and modify the activity details.

See *Modifying an activity* on page 251 for information on modifying activity details.

Creating a Jump activity

A Jump activity is used to re-route the process forward or backward to a specific activity. For example, when an approval is declined, the process may be sent back to another activity for changes or sent forward to the End activity.

To create and add a Jump activity:



- 1 Position the cursor over the Jump icon, then click and hold down the left mouse button.
- 2 Drag the Jump icon over an activity so that the new activity precedes, follows, or parallels the activity.

Notice that a rectangle outlined in red appears along with the icon.

To select the placement of the Jump activity, position the red rectangle in one of the positions described in the following table and click the left mouse button

Note: The position of the activity is determined by where the red rectangle is located when you release the mouse button.

When positioned...	The activity is placed...
over the first half of the current activity	before the current activity
over the last half of the current activity	after the current activity

When positioned...

over the top half of the current activity

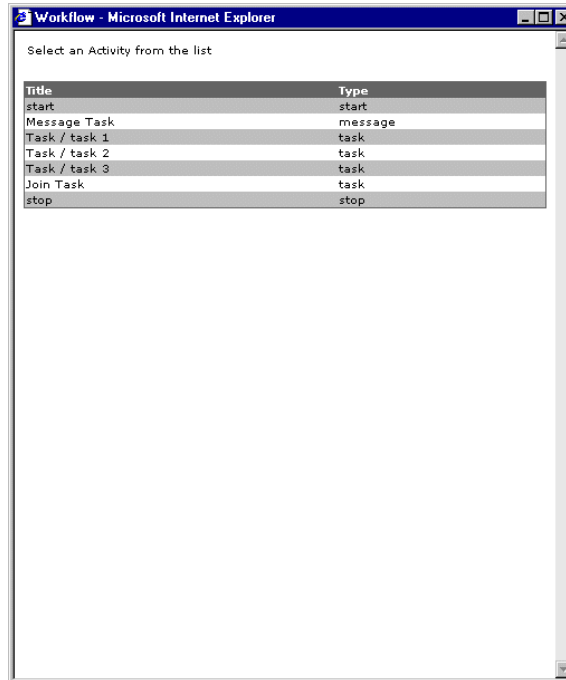
over the bottom half of the current activity

The activity is placed...

above the current activity

below the current activity

After you release the mouse button, the Workflow window appears.



- From the activity list, select the destination activity for the jump.

The title of the destination activity appears in the Screen Tip when the cursor is placed over the jump activity.

The Workflow window closes and the Jump activity is added in the workflow designer.

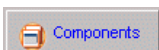
Adding a Component Template

Component templates are a set of activities that represent a portion of a process that can be used in more than one workflow template. See *Creating a Component template* on page 257.

When component templates have been pre-defined in the system, you can add them to your workflow template if they meet your requirements for the process being defined.

A component template that is added to a workflow process template is a copy and is no longer linked to the original component template. If changes are made to the original component template, a component template previously added to a workflow process template does not inherit those changes.

To add a component template:



- 1 Position the cursor over the Components icon, then click and hold down the left mouse button.
- 2 Drag the Components icon over an activity so that the component template precedes, follows, or parallels the activity.

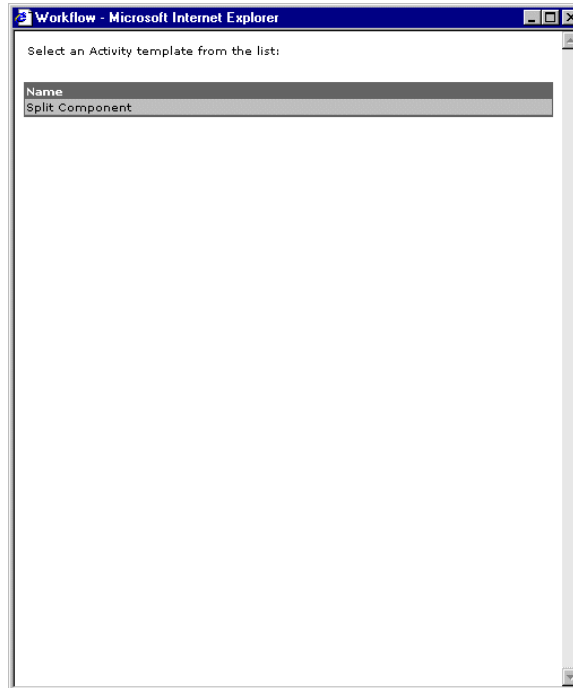
Notice that a rectangle outlined in red appears along with the icon.

To select the placement of the activity, position the red rectangle in one of the positions described in the following table and release the left mouse button.

Note: The position of the activity is determined by where the red rectangle is located when you release the mouse button.

When positioned...	The activity is placed...
over the first half of the current activity	before the current activity
over the last half of the current activity	after the current activity
over the top half of the current activity	above the current activity
over the bottom half of the current activity	below the current activity

After you release the mouse button, the Workflow window displays a list of component templates.



- 3 Click the component template you want to add to the workflow template. The Workflow window closes and the component template is added in the workflow designer.

Modifying an activity

In the process of designing a workflow template, after activities are created, they may need to be moved to another location in workflow, re-defined using different options, or renamed.

The Sample activity provided in the initial workflow designer must be modified if you want to use it within your workflow template.

Activities can be modified before or after the workflow template is saved.

Note: Modifying an activity within a workflow template that has already been created does not effect process instances that are currently running. After a process instance is started, it is no longer linked to the workflow template.

To modify an activity

- 1 Click the activity you want to modify.
The Workflow window for the selected activity displays the activity details.
- 2 Make the required modification to the activity details.
Depending on the activity you are modifying, see *Creating a new activity* on page 235, *Creating a Select activity* on page 244, *Creating a Jump activity* on page 248, or *Adding a Component Template* on page 249 for specific instructions on defining activity details.
- 3 Click Update.

Deleting an activity

Activities can be deleted from a workflow template before or after you save the workflow template.

Note: Deleting an activity within a workflow template that has already been created does not effect process instances that are currently running. After a process instance is started, it is no longer linked to the workflow template.

To delete an activity:

- 1 Using the left mouse button, click the activity you want to delete and hold down the mouse button.
- 2 Drag and drop the activity onto the Trash icon.



Saving the Workflow template

After you complete a new workflow template, you must save the template.

To save the workflow template:

- ▶ Click **Create**.
The workflow template is added to the **List of Workflow templates**.

Note: If you exit the **Create a New Workflow** page prior to clicking **Create**, all changes to the workflow template are discarded.

Creating a workflow template from another template

A workflow template can be created from a defined workflow template that has many of the same activity sequences.

To create a workflow template from another template:

- 1 Log on to your Web application to display the Navigation Menu on your Home page.
- 2 Click the Workflows tab, or click **Workflows** from the Navigation Menu.
The Workflow menu appears in the left pane.
- 3 Click **Template Design** from the Workflows left pane menu to display the **List of Workflow templates** page.
- 4 Locate and click the name of the workflow template you want to use as the base for the new workflow template.
The **Details for template** page appears.
- 5 Make modifications to the template to accommodate the required activities for the new template.
See *Creating a workflow template* on page 230 for information on adding, modifying, or deleting activities.
- 6 Change the name of the template.
- 7 Click **Save As** to save the workflow template with the new name.

Modifying a Workflow template

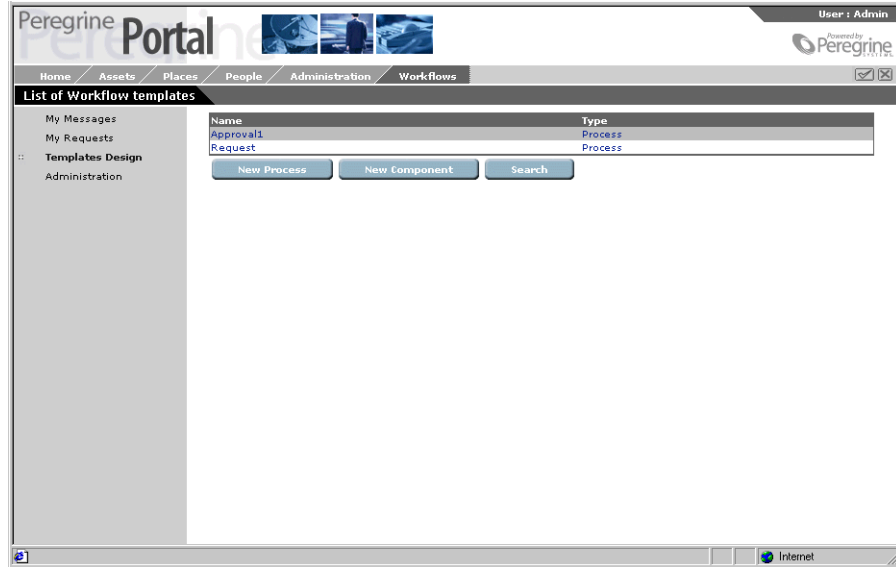
A workflow template can be modified as necessary to ensure its continued alignment with the business process it represents.

Note: Modifying a workflow template does not affect process instances that are currently running. After a process instance is started, it is no longer linked to the workflow template.

To modify a workflow template:

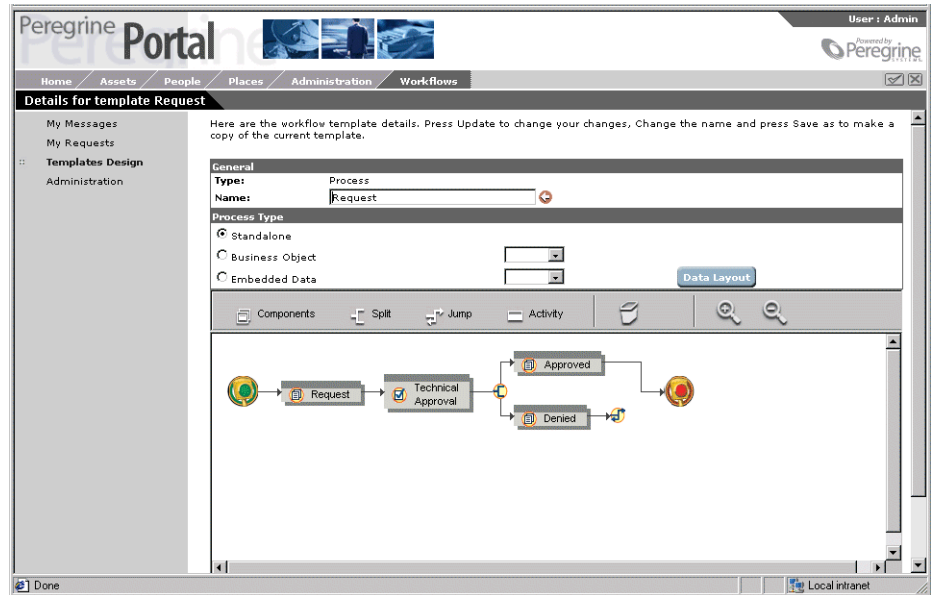
- 1 Log on to your Web application to display the Navigation Menu on your Home page.
- 2 Click the Workflows tab, or click **Workflows** from the Navigation Menu.
The Workflow menu appears in the left pane.

- 3 Click **Templates Design** from the Workflows left pane menu to display the **List of Workflow templates** page.



- 4 Locate the workflow template you want to modify.
- 5 Click the name of the workflow template you want to modify.

The Details for template page appears.



6 Make the necessary modifications to the template.

See *Creating a workflow template* on page 230 for information on adding, modifying, or deleting activities.

7 Click Update to update the workflow template and return to the List of Workflow templates page.

Deleting a Workflow template

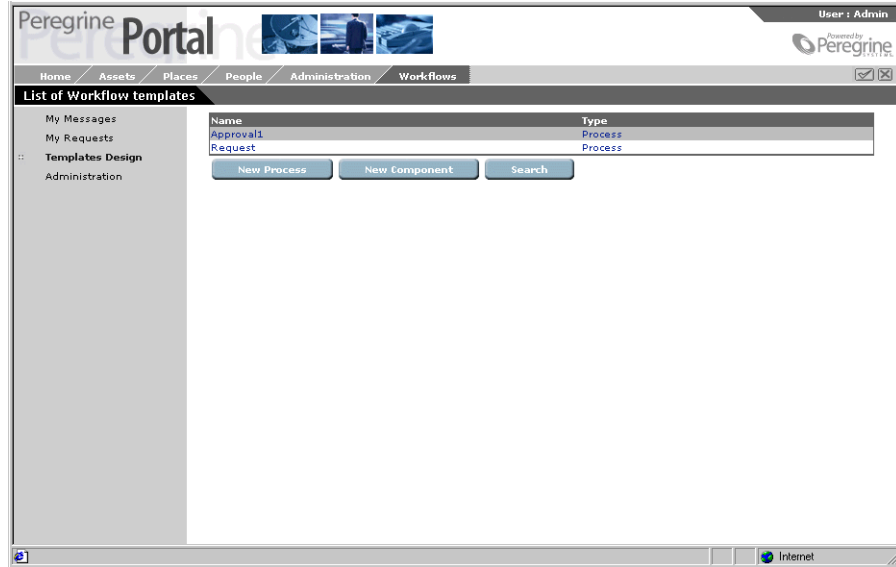
When a workflow template is no longer useful or the process has been redefined as another template, you can delete the workflow template.

Note: Deleting a workflow template does not effect process instances that are currently running. After a process instance is started, it is no longer linked to the workflow template.

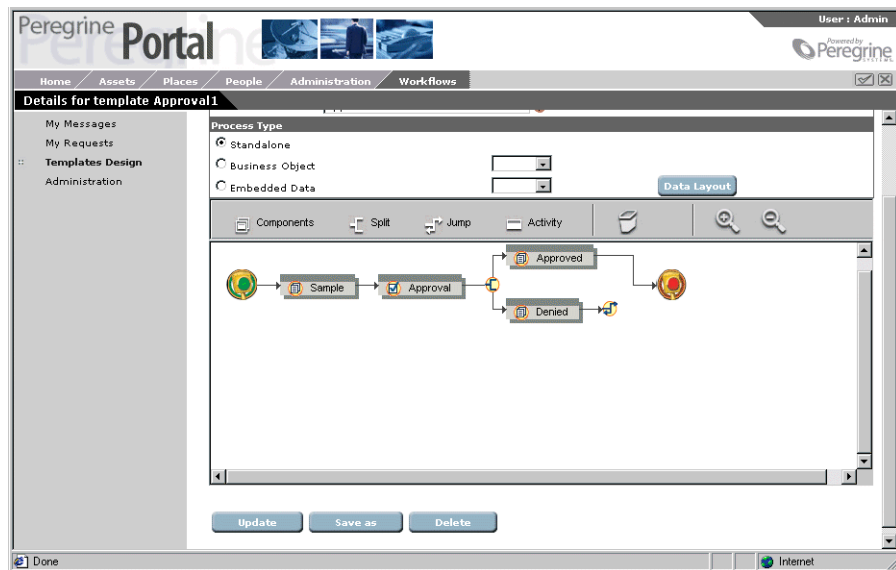
To delete a workflow template:

- 1 Log on to your Web application to display the Navigation Menu on your Home page.
- 2 Click the Workflows tab, or click **Workflows** from the Navigation Menu. The Workflows menu appears in the left pane.

- Click **Template Design** from the Workflows menu to display the **List of Workflow templates** page.



- Locate the workflow template you want to delete.
 - Click the name of the workflow template you want to delete.
- The **Details for template** page appears.



- 6 Scroll to the bottom of the page, and then click **Delete** to delete the workflow template and return to the **List of Workflow templates** page.

The workflow template list no longer displays the name of the deleted workflow template.

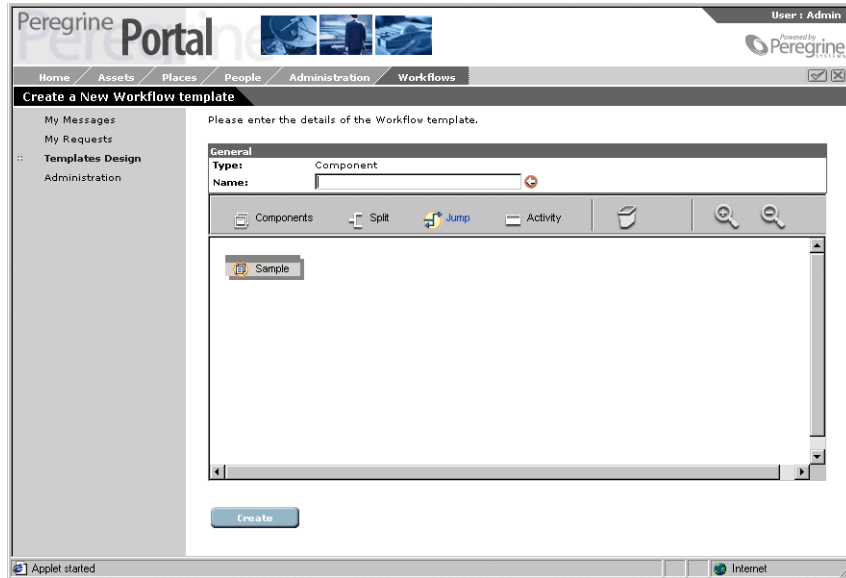
Creating a Component template

Component templates are a set of activities that represent a portion of a process. These templates can be used when designing workflow process templates.

To create a component template:

- 1 Log on to your Web application to display the Navigation Menu on your Home page.
- 2 Click the Workflows tab, or click **Workflows** from the Navigation Menu. The Workflow menu appears in the left pane.
- 3 Click **Template Design** from the Workflows left pane menu to display the **List of Workflow templates** page.
Note: After component templates are defined, the template name and type (Component), appears in the list.
- 4 Click **New Component**.

The Create a New Workflow template page opens.



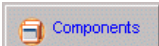

- 5 In the Name text box, type the name of the new component template.




The component template defines a specific set of activities. The name assigned to the template *must* be unique.

Notice that the workflow designer contains only a sample activity. Since a component template is designed to be added to a workflow template, component templates do *not* contain the Start and End activities.



The sample activity can be modified for use in the component template or deleted. See [Modifying an activity](#) on page 251 and [Deleting an activity](#) on page 252.

- 6 In the workflow designer, create and add activities to the component template using the toolbar icons described in the following table.

Icon	Description
	Select a new activity from the template list. See To add a component template : on page 250 for information on adding an activity from the template list.
	Create a new Select activity. See To create and add a Select activity : on page 245 for information on adding a Select activity.

Icon	Description
	Create a new Jump activity. See <i>To create and add a Jump activity</i> : on page 248 for information on adding a Jump activity.
	Create a new activity. See <i>To create and add a new activity</i> : on page 235 for information on adding a new activity.
	Trash. See <i>To delete an activity</i> : on page 252 for information on deleting an activity from a workflow template.

In addition to the activity icons on the toolbar, zoom functionality is provided by the following toolbar icons.

Icon	Description
	To zoom in on the workflow template graphic, click the Zoom in icon until the required magnification is achieved.
	To zoom out on the workflow template graphic, click the Zoom out icon.

To create and add a new activity, see *Creating a new activity* on page 235. To create and add a Jump activity, see *Creating a Jump activity* on page 248. To create and add a Select activity, see, *Creating a Select activity* on page 244. To add a component template for inclusion into this component template, see *Adding a Component Template* on page 249.

See *Modifying an activity* on page 251 and *Deleting an activity* on page 252 for information on modifying and deleting activities.

7 Click Create.

The component template is added to the **List of Workflow templates**.

Note: If you exit the **Create a New Workflow** page prior to clicking **Create**, all changes to the workflow template are discarded.

Using Workflow Administration

This section explains the functions available in Workflow Administration activity. The functions described include:

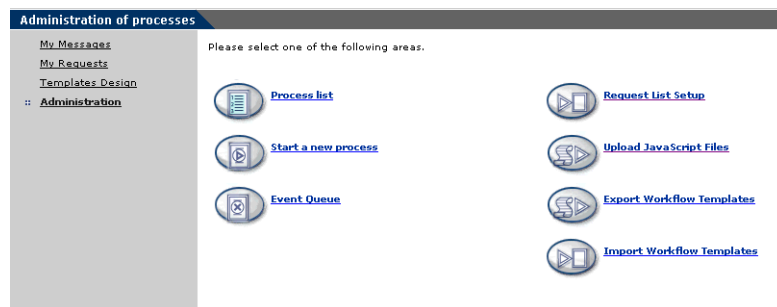
- *Accessing the Administration function* on page 260
- *Monitoring process instances* on page 261
- *Updating a process instance* on page 262
- *Starting a new process instance* on page 264
- *Viewing the Event Queue* on page 267
- *Setting Up the Request List* on page 268
- *Uploading JavaScript Files* on page 275

Accessing the Administration function

The workflow administration functions can be accessed only by users having the required capabilities (permissions).

To access the Administration function:

- 1 Log on to your Web application to display the Navigation Menu on your Home page.
- 2 Click the Workflows tab or click **Workflows** from the Navigation Menu. The Workflows links appear in the left pane.
- 3 Click the **Administration** link display the **Administration of processes** form.



From this page you can select the following areas of administration:

- Process list
- Start a new process

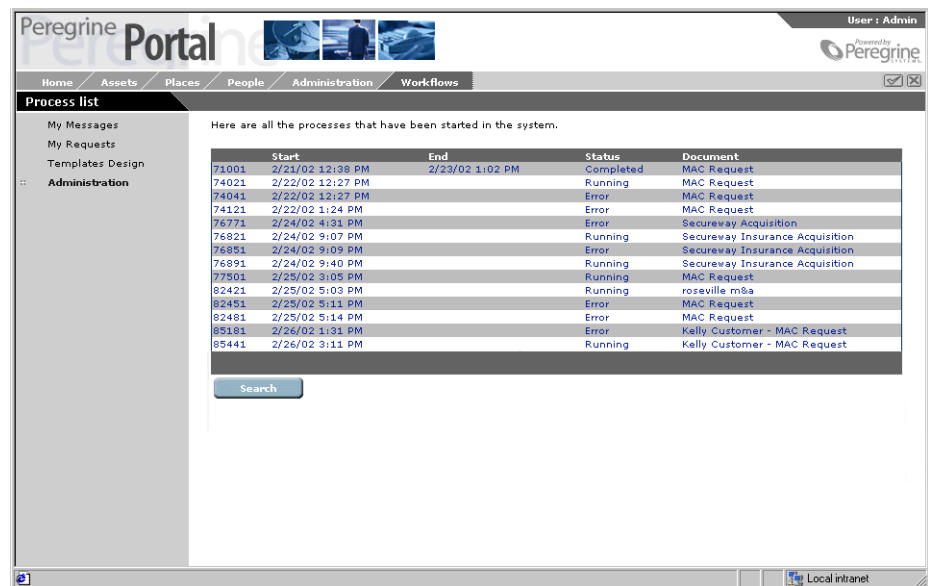
- Event queue
- Request List Setup
- Upload JavaScript Files
- Export Workflow Templates
- Import Workflow Templates

Monitoring process instances

Using the **Process list** administration function, you can monitor the status of all process instances started in the system.

To view the process list:

- 1 From the **Administration of processes** page, click **Process list**.
The **Process list** page opens.



The screenshot shows the Peregrine Portal Administration interface. The 'Process list' window is open, displaying a table of process instances. The table has the following columns: Reference, Start, End, Status, and Document. Below the table is a search button.

Reference	Start	End	Status	Document
71001	2/21/02 12:08 PM	2/23/02 1:02 PM	Completed	MAC Request
74021	2/22/02 12:27 PM		Running	MAC Request
74041	2/22/02 12:27 PM		Error	MAC Request
74121	2/22/02 1:24 PM		Error	MAC Request
76771	2/24/02 4:31 PM		Error	Secureway Acquisition
76821	2/24/02 9:07 PM		Running	Secureway Insurance Acquisition
76851	2/24/02 9:09 PM		Error	Secureway Insurance Acquisition
76891	2/24/02 9:40 PM		Running	Secureway Insurance Acquisition
77501	2/25/02 3:05 PM		Running	MAC Request
82421	2/25/02 5:03 PM		Running	roseville m&a
82451	2/25/02 5:11 PM		Error	MAC Request
82481	2/25/02 5:14 PM		Error	MAC Request
85181	2/26/02 1:31 PM		Error	Kelly Customer - MAC Request
85441	2/26/02 3:11 PM		Running	Kelly Customer - MAC Request

A list of all processes started in the system opens in the **Process list** window. The list contains the following columns of information about the associated process instance:

- Reference—The reference number assigned to the process instance.
- Start—The date the process instance was started.
- End—The date the process instance was completed.

Status—The current status of the process instance (Timed out, Completed, Running, Error).

Document—A description of the process instance.

- 2 If you want to sort the list according to a particular column attribute, click on the heading of that column.
- 3 If you do not see the specific process instance you are looking for or if you want to search by specific criteria, click **Search**.

The Template Search page opens.

The screenshot shows a search interface with the following elements:

- General** section:
 - Process or document name:** A text input field.
 - Requester:** A field with two user selection icons.
 - Process start date:** A field with four date pickers and a time separator.
 - Process status:** A dropdown menu.
- This is an advanced option.** section:
 - Business object:** A dropdown menu.
- Perform Search** button.

- 4 Enter your search criteria in the fields provided, and then click **Perform Search**.

A list of the processes matching your search appears.

- 5 Click **Search** again to rerun your search, or click the **Administration** link to return to the Administration of processes page.

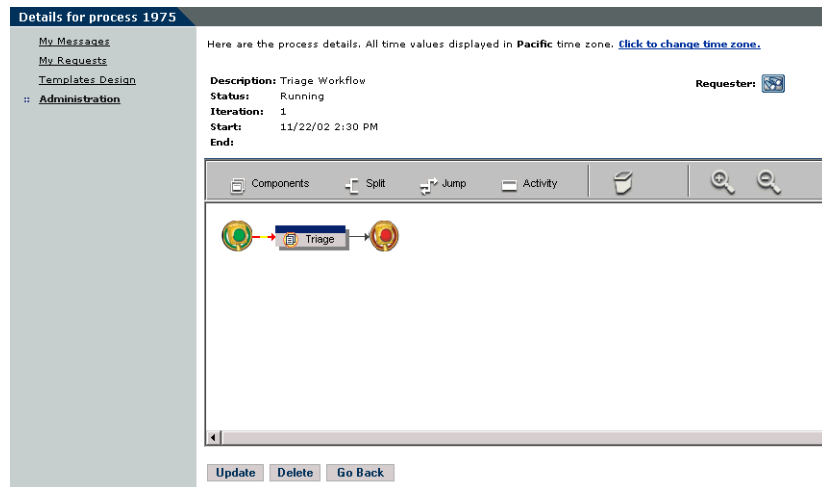
Updating a process instance

A process instance can be updated through the **Details for process** page. The most common reason to update a process instance is that an error has occurred during routing and the process instance has stopped.

Important: After you update a process instance because an error occurred, use the procedure in *Viewing the Event Queue* on page 267 to locate the process instance error and restart the process instance.

To update a process instance:

- 1 From the **Administration of processes** page, click **Process list** to display the **Process list** page.
- 2 If you want to sort the list according to a particular column attribute, click on the heading of that column.
- 3 Use the process instance Reference number to locate the process instance you want to update, or click **Search** to search for existing work processes.
- 4 Click the process instance to display the **Details for process** page for the selected process instance.



- 5 Make the necessary changes to the process instance activities.
 - Note:** You cannot change a process instance activity that has already been processed.
- 6 Click **Update** to apply the changes and return to the **Process list** page.

Deleting a process instance

Documents within the knowledgebase are associated with a workflow process instance. When these documents are created, a process instance is started. Even when a document is deleted, the process instance continues, which means task messages might be sent to users on the system. These messages may be distributed to the user assigned a task, as well as all users with the same role.

After a document is deleted, the process instance associated with the deleted project or contact must also be deleted.

To delete a process instance:

- 1 From the Administration of processes page, click **Process list** to display the Process list page.
- 2 Use the process instance reference number to locate the process instance you want to delete.
- 3 Click the process instance to display the Details for process page for the selected process instance.

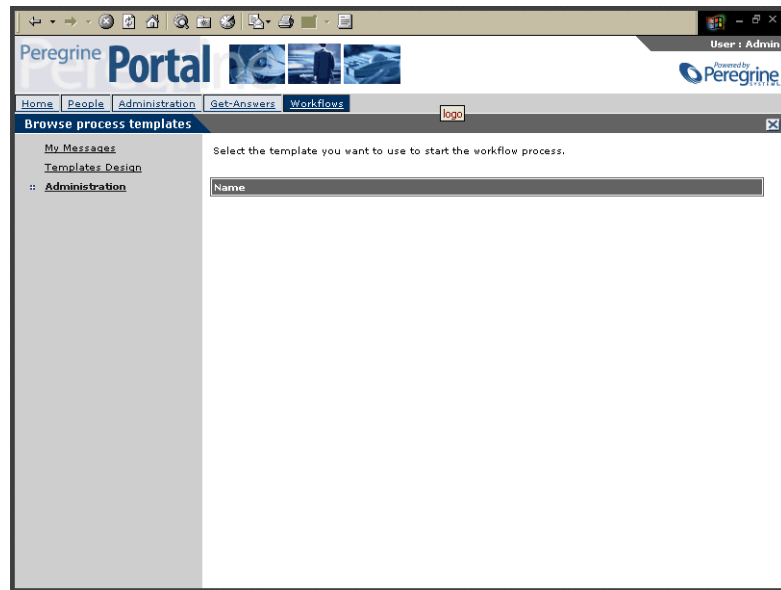
- 4 Click **Delete** to delete the process instance and return to the Process list page.

Starting a new process instance

You can manually start processes that are not related to projects or contracts using the **Start a new process** administration function.

To start a process instance:

- 1 From the Administration of processes page, click Start a new process to display the Browse process templates page.



- 2 From the list of templates, select the template you want to use to start the workflow process.

The Process submit page opens.

The screenshot shows the 'Process submit' page in the Peregrine Portal. The page header includes the 'Peregrine Portal' logo and the user name 'Admin'. The navigation menu shows 'Administration' as the active section. The main content area contains a 'Parameters' section with the following fields:

- Start Date:** A date picker showing 'May 20 2002' and a time picker showing '9 : 24 AM'.
- Description:** A text input field.

A 'Submit' button is located below the 'Description' field. The page also includes a sidebar with 'My Messages', 'My Requests', and 'Templates Design' options, and a footer with 'Local intranet'.

- 3 In the Start Date fields, select the date and time that you want the process to start. You can use either the drop-down lists by each field, or click the calendar to select a date.
- 4 In the **Description** text box, type a description for the new process instance.
- 5 Click **Submit**.

The **Process submitted** page opens.



The process number assigned to the new process appears in the **Process information** frame. Note the process number.

- 6 Click **Continue** to return to the **Administration of processes** page.

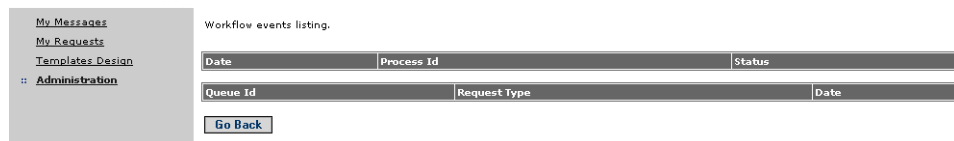
Viewing the Event Queue

The Workflow Event Queue is made up of two queues:

- **Internal** - events occurring within the OAA workflow engine. These events have a Process Id. They are listed in the first section on the Event Queue page.
- **External** - events started outside the OAA workflow engine. Examples include Notification Services events. These events have a Queue Id. They are listed in the second section of the Event Queue page.

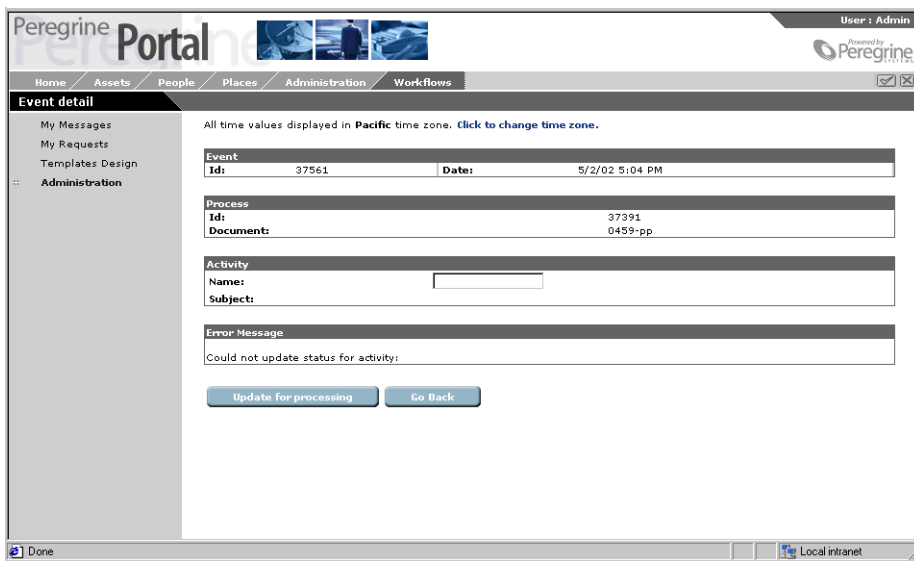
To view events:

- 1 From the **Workflows** page, click **Event Queue**.



- To view the details of an event, click any of the column entries associated with that event.

The **Event detail** page opens.



- After reviewing the error information, you can do one of the following:
 - Click **Update for processing** to restart processing.
 - Click **Go Back** to return to the **Event Queue** page.
 - Click **Edit Process** to go the process instance and correct the issue.

Setting Up the Request List

The Request List is a collection of request definitions that process a specified workflow template. A workflow template of any process type can be used for the request definition. However, when the process type is Embedded Data, the data is embedded in the workflow process. For example, a request list definition could be used to order business cards for employees, or to process change of address requests. When the workflow process type is Embedded Data, the employee information data is available to each workflow activity.

A request definition can be used to provide various request functions. However, you may need a programmer to write specific scripts that provide the functionality required by your request definitions.

After the system creates a request definition for the request list, a user who has the required capabilities can view the list and create new requests through My Requests.

Searching for a Request Definition

The **Request Search** page provides search functionality. You can search using the available text box. To narrow the search, provide as much information as possible.

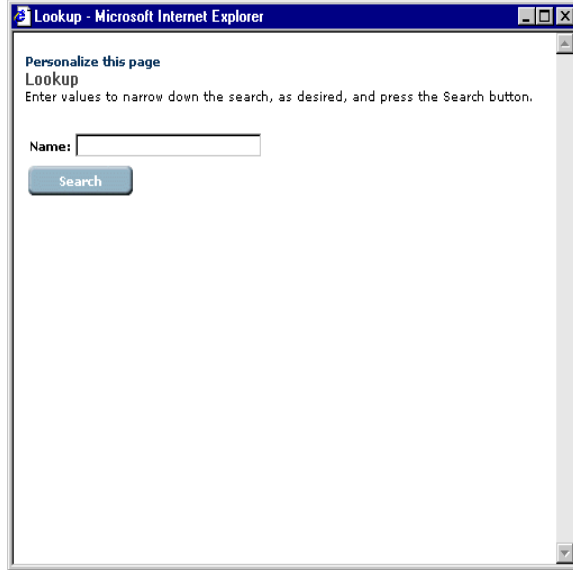
To search for a request definition:

- 1 From the **Administration of processes** page, click **Request List Setup** to display the **Request Search** page.

The screenshot shows the 'Request Search' page in the Peregrine Portal. The page has a header with the logo and user information. A navigation bar is present below the header. The main content area is titled 'Search' and contains a search form. The form has a 'Name' text box, a 'Workflow Template' dropdown menu, and three buttons: 'Search', 'View All', and 'New'. The search form also includes a 'Please enter the search criteria and press the Search button.' instruction.

- 2 Type the request definition name in the **Name** text box.
If you know part of the name, you can type it between% (percent) signs.

- 3 Click the **binoculars** icon next to Workflow Template to display the Lookup Contact Phone window.



Lookup - Microsoft Internet Explorer

Personalize this page

Lookup

Enter values to narrow down the search, as desired, and press the Search button.

Name:

Search

- 4 Using this window, locate and select the workflow template.
- 5 Click **Search** to filter the list of request definitions and display only those matching the search criteria.



Peregrine Portal

User: Admin

Home Assets People Places Administration Workflows

Search Results

Please click on any item to view it in detail.

Name	Workflow Template
Move Request	MAC Request
Workflow Template	

New Search New

Local intranet

Note: You can sort the search results list by any of the displayed columns. To sort the list, click the column title.

The **Request Search Results** page displays only the request definitions matching the search criteria. From the list, you can access the details for a request definition by selecting one of the column entries for a specific request definition. The **Request Details** page displays the details for the selected user.

To view all request definitions defined in the system:

- ▶ Click **View All**.

To perform a new search:

- ▶ From the **Request Search Results** page, click **New Search** to display the **Request Search** page.



Setting Up a New Request Definition

Use the following procedures to define, modify, or delete request definitions.

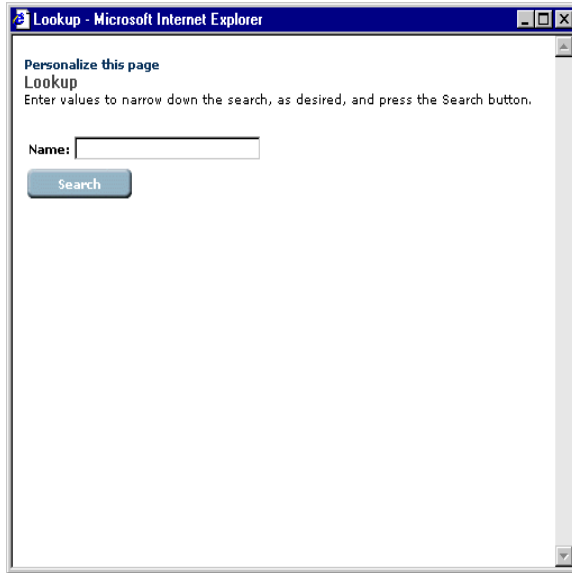
To set up a request definition:

- 1 From the **Administration of processes** page, click **Request List Setup** to display the **Workflows Request Search** page.
- 2 Click **New**.
- 3 The **Create New Request** page opens.

Please fill in the requested information and click the submit button.

Identification	
Name:	<input type="text"/>
Icon:	<input type="text"/>
Workflow Process	
Workflow Template:	
Startup Options for Embedded Data Process Type	
Show Startup Screen:	<input type="checkbox"/>
Startup Script:	
Security	
Capabilities required:	<input type="text"/>
<input type="button" value="Submit"/> <input type="button" value="Go Back"/>	

- 4 Type a name for the request definition in the **Name** text box.
- 5 Type the path for the icon in the **Icon** text box.
- 6 Click the **binoculars** icon next to Workflow Template to display the Lookup Workflow Template window.



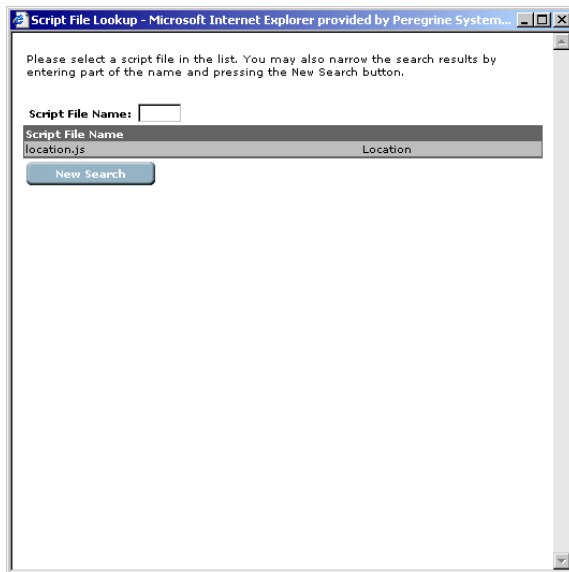
- a Using this window, define your search criteria.
- b Click Search.

The Lookup Workflow Template window displays a list of all workflow templates matching the search criteria.



- c From the list, select the workflow template to associate with the request definition.
- 7 Select the **Show Startup Screen** check box if the workflow template was created as an Embedded Data process type.
See *To create a workflow template:* on page 231.

- 8 Click the search icon next to Startup Script to display the Script File Lookup window.



- 9 Locate and select the script file you want to use.
- 10 To add a capability, type the capability in the **Capabilities required** text box.

Important: The user must be assigned a role with that capability.

- 11 Click **Submit**.
The Workflow Request Details page opens and displays the information you have entered.
- 12 Click **Submit Changes**.

Modifying a Request Definition

Request definitions can be modified using the Workflow Request Details page.

To modify a request definition:

- 1 To search for the request definition you want to modify, see *Searching for a Request Definition* on page 269 for information on using the search function.
- 2 Select the request definition from the Request Search Results page to display the Workflow Request Details page.

The Workflow Request Details page displays the information for the request definition you selected.

- 3 Make any changes to the request definition information.
- 4 Click **Submit** to save all changes to the request definition information.

Deleting a Request Definition

Request definitions can be deleted from the system through the Workflow Request Details page.

To delete a request definition:

- 1 To search for the request definition you want to delete, see *Searching for a Request Definition* on page 269 for information on using the search function.
- 2 Select the request definition from the Request Search Results page to display the Workflow Request Details page.

The Workflow Request Details page displays the information for the request definition you selected.

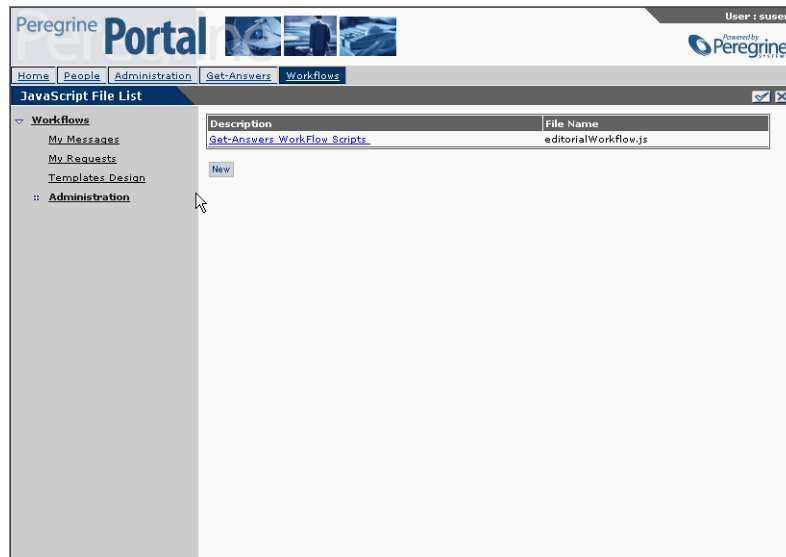
- 3 Click **Delete**.
A delete confirmation message appears.
- 4 Click **OK** to delete the request definition from the system.

Uploading JavaScript Files

JavaScript files must be uploaded to the server before they can be assigned to a workflow process activity. Use the following procedures to upload all JavaScript files you want to make available for use in your workflow templates.

To view uploaded JavaScript files:

- 1 From the **Administration of processes** page, click **Upload JavaScript Files** to open the JavaScript File List page.



A list of all script files that have previously been uploaded to the server appears. The list contains the following columns of information about the script file:

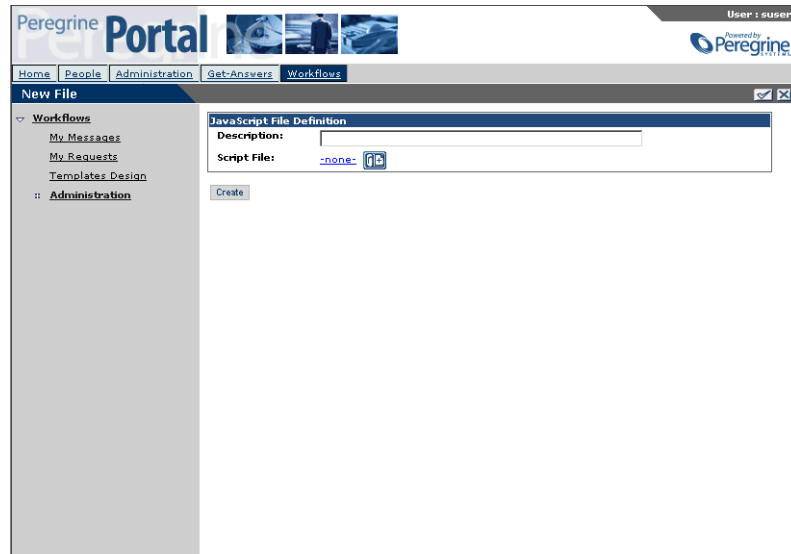
Description—A description of the script file function.

File Name—The name of the script file.

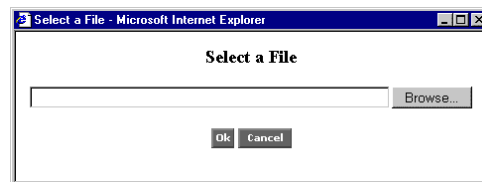
- 2 To view the script file details, click the entry in the description column for the JavaScript file you want to review.

To upload a new script file:

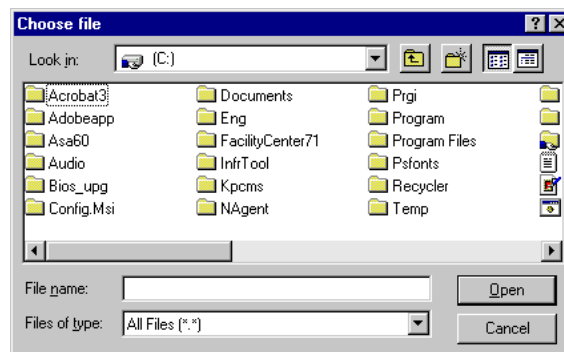
- 1 From the JavaScript File List page, click New to display the New File page.



- 2 Type a description of the script file in the Description text box.
- 3 Click the Plus icon to display the Select a File window.



- 4 Use the Browse button to display the Choose file window.



- 5 Locate and select the script file to upload.
- 6 Click OK.
The Script File entry displays the selected file name.
- 7 Click **Create** to save the new script file.
The JavaScript File List page displays the new script file in the list.

Updating a Script File

A script file can be updated through the Update File page.

Warning: Use caution when updating a script file. Changing the information may produce unwanted or unexpected results.

To update a file:

- 1 From the JavaScript File List page, select the file you want to update.
The Update File page appears.



- 2 Make any required changes in the **Description** text box.
- 3 If you want to add a new file attachment, click the Plus icon to display the Select a File window and add a new file attachment.
- 4 Click **Save** to save the changes and return to the JavaScript File List page.

Deleting a Script File

Script files can be deleted from the system through the Update File page.

Warning: Use caution when deleting a script file. Deleting a script file that is used in conjunction with a workflow may produce unwanted or unexpected results.

To delete a script file:

- 1 From the JavaScript File List page, select the file you want to delete.
The Update File page appears.
- 2 Click **Delete**.
A delete confirmation message box opens.
- 3 Click **OK** to confirm the delete and return to the JavaScript File List page.

Importing/Exporting Workflow Templates

Workflow templates can be moved from one Get-Answers installation to another. It is as simple as exporting them from one system and importing them to another

To Export:

- 1 In Get-Answers, click the **Workflows** tab.
- 2 Click the **Administration** link.

The Administration of processes page opens.

- 3 Click **Export Workflow Templates**.

The Export Workflow Templates page opens.

Workflow Templates
Select templates to export.

Available Templates	Current Selection
<ul style="list-style-type: none"> \$\$\$IDS(a,a) Editorial Workflow Triage Workflow 	

Export Options
Specify the file path on the server in which the export files are to be placed. Select the objects that are referenced in the template activities.

Export File Path:

Subprocess: Export subprocesses referenced in activities

NS Custom Template: Export notification custom templates used in activities

Role: Export roles referenced in role assignments

Script: Export script files used in script activities

- 4 In the **Available Templates** list on the left, double-click the templates you want to export.
They appear in the **Current Selection** box.
- 5 In the **Export Options** section, type the **Export File Path** for the exported templates.
- 6 Click the **Subprocess**, **NS Custom Template**, **Role**, and **Script** check boxes to include these elements in the export, if applicable.
- 7 Click **Submit**.


A confirmation message appears in the Workflow Export Results page that opens. Be sure to note the location on the server where the files were saved.

To Import:

- 1 In Get-Answers, click the **Workflows** tab.
- 2 Click the **Administration** link.
- 3 Click **Import Workflow Templates**.

The Import Workflow Data page opens.


Import Options
Specify the file path on the server where the import files are placed.

Import File Path: 

- 4 In the **Import Workflow Data** file page that opens, enter the path to the workflow template(s) you want to import, and then click **Next**.

The Import Workflow Data page re-opens with the files and scripts you have selected to import listed.

Import Options
Specify the file path on the server where the import files are placed. Select the objects that are to be imported.

Import File Path: 

Document files found in import directory:

NSTemplate.xml
WfwJSFile.xml
WfwRole.xml
WfwTemplate.xml

Script files found in import directory:

- 5 Verify the **Files in the import directory** are correct and click **Start Import**.
A message informs you that the Import completed.
- 6 To verify the import, click **Templates Design**.
The Templates appear in the list. See *Modifying a Workflow template* on page 253 for details about modifying a template.

Using the Request List

The My Requests Request activity lists requests for the admin user currently logged in. This section explains how to view request definitions, start a new request workflow, and view overdue requests.

Accessing My Requests

Use the following procedure to access My Requests.

To access My Requests:

- 1 Log on to your Web application to display the Navigation Menu on your Home page.
- 2 Click the **Workflows** tab or click **Workflows** link.
The My Messages page opens.
- 3 Click **My Requests** to display the My Requests page.



Viewing Request Details

Use the following procedure to view the details of a request.

To view the request details:

- 1 In the description column, click the description for the request you want to review.

The detailGeneral page opens.

The screenshot shows the 'detailGeneral' page in the Peregrine Portal. The page is divided into a left sidebar and a main content area. The sidebar contains a 'Workflows' section with sub-links for 'My Messages', 'My Requests', 'Templates Design', and 'Administration'. The main content area has two tabs: 'General' and 'Workflow'. The 'General' tab is active and displays the following information:

- General**
 - Status: Running
 - Iteration: 1
 - Start: 6/13/03 2:05 PM
 - End: (blank)
- Description**
 - Triage Workflow
- History**

Start Date	End Date	Subject	To	Status
6/13/03 2:05 PM		defect	user, super (Owner)	In progress

At the bottom of the page, there is a button labeled 'Return To Request List'.

This General tab displays general information about the request, the request description, and the request process history. The Workflows tab displays the workflow template used for this process instance.

From the Workflows tab you can modify the process workflow. See *Modifying a Workflow template* on page 253.

- 2 On the General tab, click **Return to Request List**, to re-display your request list.

Initiating a New Request

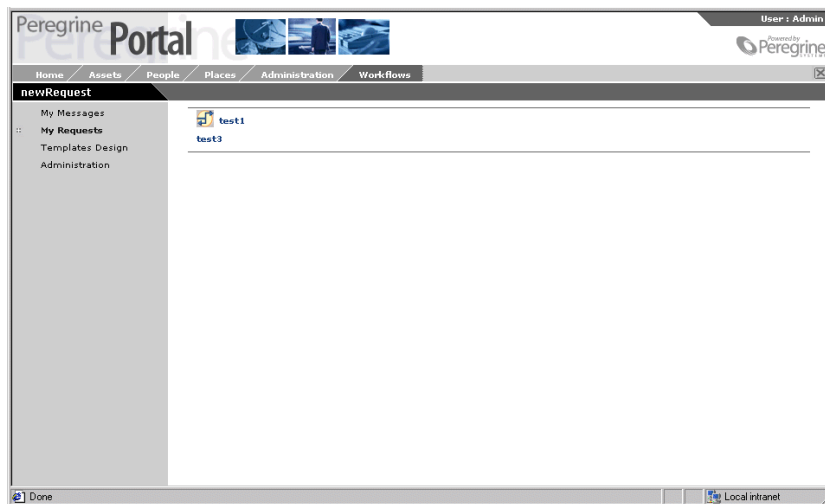
Use the following procedure to initiate a new request.

Note: Before any system users can initiate a new request, there must be at least one workflow for a New Request Definition available. See *Setting Up a New Request Definition* on page 271.

To initiate a new request:

- 1 From the My Requests page, click New Request.

The New Request page opens.



- 2 Click on the request you want to initiate.

The workflow process instance for the request appears in the request list of your My Requests page.

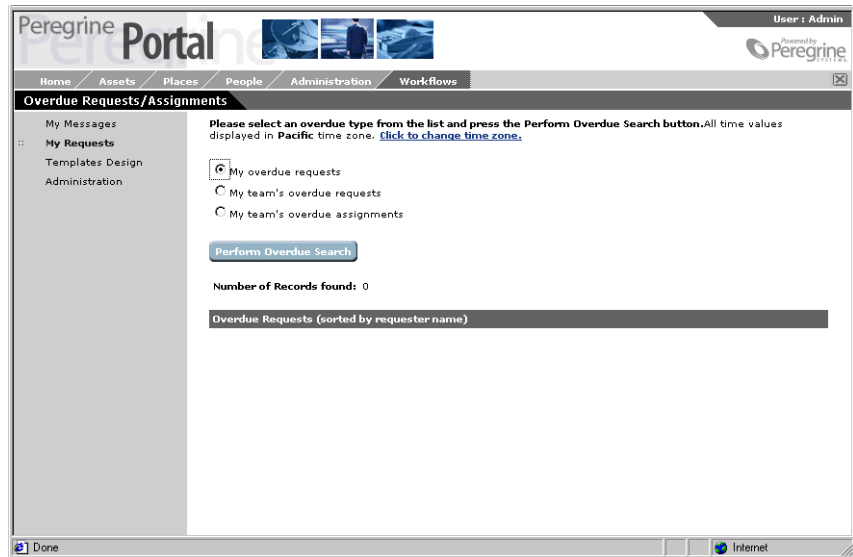
Viewing Overdue Requests

Use the following procedure to view overdue requests.

To view your overdue requests:

- 1 From the My Requests page, click **My Overdue Requests**.

The Overdue Requests/Assignments search page opens. It displays a list of your overdue requests.



Note: Times appear according to the time set in your Change Time Zone Preference page. To change to another time zone, from the Home tab, click the **Click to change time zone** link, select a time zone, then click **Submit**.

- 2 Click the search icon next the the overdue request to view the details of a request.
The detailGeneral page opens and displays the details of the request.
- 3 If you want to view your team's overdue requests or assignments, select the appropriate option button.
- 4 Click **Perform Overdue Search**.

The **Overdue Request/Assignments** page displays the information you requested.

Admin Settings for Workflow

- 1 Log on with an administrator role.
- 2 Click the **Administration** tab.
The Control Panel page opens.
- 3 Click **Settings**.
The Admin Settings page opens.
- 4 Click the **Workflow DB** tab.
- 5 Read the instructions on the page. Determine the settings you need to change (if any). Make the changes.
- 6 Click **Save**.
The Control Panel appears.
- 7 Click **Settings**.
- 8 Click the **Workflow Engine** tab.
- 9 Read the instructions for each field. Determine the settings you need to change (if any). Make the changes.
- 10 Click **Save**.
The Control Panel appears.
- 11 Click **Reset Server**.
A message informing you that the server reset was successful appears at the top of the page. The Administration Settings related to Workflow are now configured.

11 Importing Legacy Data

CHAPTER

This chapter explains how to:

- Format data from other applications, such as Tivoli ServiceDesk or Knowlix, to the Get-Answers format.
- Import the data into the Get-Answers database.

For data from applications other than Knowlix, you must create an application that converts the data into the Get-Answers XML format. See *Converting legacy data* on page 288 for an explanation of the format and folder structure your data must take.

For Knowlix data, you can use a conversion utility available from Peregrine Systems to convert and structure the data. To do this, you must have purchased a license to upgrade from Knowlix to Get-Answers. See *Converting Knowlix data* on page 301 for more information.

Once you have converted your data, use Get-Answers to import it to the Get-Answers database. See *Importing your data to Get-Answers* on page 303 for more information.

When you have completed the steps in this chapter, you can customize the data you imported using Get-Answers' Document Types and Views, which are described earlier in this guide. See *Chapter 12, Document Types and Views*. For the converted and/or imported data you may need to:

- Add new views for any new document types created by importing data.
- Add input forms for the new document types.

- Add edit forms for the new document types.
- Add new fields from the new document types for searching.

Converting legacy data

To take data from applications such as Tivoli ServiceDesk and format it so that you can use it in Get-Answers, you must create an application that converts your data to XML. This section explains how you must structure your files for the conversion.

To structure your files for conversion:

- Step 1** Create an XML export file for each legacy document you want to import to Get-Answers.
- Step 2** Create a directory structure for each XML export file based on its category or subcategory.
- Step 3** Create a single directory for attachments. This directory holds all the supporting files for the documents.
- Step 4** Backup your directories.
- Step 5** Import data.
- Step 6** Move the generated search engine fields for indexing.
- Step 7** Create a new document type view for each document type you imported. See *Chapter 12, Document Types and Views*.

Important: The first three steps of these procedures do not apply to migrating Knowlix data to Get-Answers. For these procedures, see *Converting Knowlix data* on page 301.

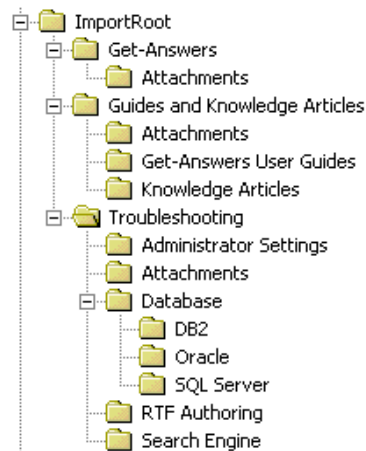
Overview

Create a folder on the Get-Answers server, for example, ImportRoot. In this folder, order is important. When importing the legacy documents to Get-Answers, the top-most folder is the one that you specify in the Import Documents page, which is in *Importing your data to Get-Answers* on page 303.. The names of the folders directly under ImportRoot will be the names of top-level categories in Get-Answers.

Note: If the top-level category name already exists in Get-Answers under any document ownership team, a new top-level category will not be created. The existing top-level category will be the one used when you import the documents in the file structure beneath the top-level category. Thus, in the case of existing top-level categories, one import operation may be run to import documents for many document ownership teams. If a top-level category does not exist, it is created under the document team selected in the Import Documents screen. If you do not select a document ownership team, the system does not create new top-level categories.

To mirror your knowledgebase categories, create a set of subfolders in a hierarchy beneath the ImportRoot folder. Do this for each set of document category hierarchies that you want to import. When importing to Get-Answers, the top-level folders under this ImportRoot folder become top-level categories. Convert levels within your knowledgebase to subfolders; these become subcategories in Get-Answers.

In this example, the names of the three folders directly under ImportRoot will be the names of top-level categories that will be created in Get-Answers if they do not already exist. Each top-level folder may have an Attachments folder under it to hold those images or documents that are shared within the document team that owns the top-level category.



Each subfolder under a top-level category folder such as Troubleshooting will be created as a subcategory during the Import Document processing. In the example above, the top-level category named Troubleshooting has four subcategories, and Troubleshooting's subcategory named Database has three subcategories.

Note: The maximum number of characters in the name of a category is 32. You can alter the database to increase this limit. The database column that holds the top-level category is *KmDomain.Name*. Subcategory names are stored in the column, *KmDomainCategory.Name*. Alter both columns to increase the number of characters in a category.

Within each folder in your newly created hierarchy, place the documents that belong in that category. Examine the folder structure of your knowledgebase carefully to remove or consolidate any folders with very few documents in them. If one category has dozens of documents and two other categories on the same level have only a few documents, consider merging some of the categories, and combining the document sets into fewer categories to simplify the presentation to the end user and to shorten the amount of time it takes to download and display hundreds or thousands of categories.

Important: The files in these folders are deleted when they are successfully imported. Make a backup copy.

For a single import

To prepare for a single import, you may want to create the document ownership teams and the categories those teams manage before you import. Once you have imported, you cannot change the team that manages the category that the documents are imported to. Nor are you able to quickly remove all the documents from a category unless the number is relatively few. Only a document team owner can set up a category to be managed by their team.

When you do that, make sure the category names match the directory names (that the document will import from) exactly, following the category naming restrictions.

Varieties of documents to import

Three varieties of documents can be placed in a folder:

- 1 Externally created documents such as .txt, .pdf, doc, .html, .xml, etc.
- 2 The .xml documents that contain metadata fields (title, summary, etc) for the externally created documents in 1.
- 3 .xml 'authored' documents of a given document type, such as Problem/Solution, Error Message/Cause, etc, or any document type that exists within your company.

Note: How to create the document views to display the data in a document type is covered in *Chapter 12, Document Types and Views*. You first import the documents for a given document type so that all the possible fields in a document are known, and then you create the document view to display the particular subset of fields for that document type.

Externally created documents

If an externally created document (1) has an .xml extension, it does not contain a <rKmDocument> element.

This is an example of an externally created document:

A text file named `readme.patch.txt` placed in the Troubleshooting folder.

.XML documents with metadata

All .xml documents that contain metadata fields (2) have an .xml file extension and contain these elements at a minimum:

```
<?xml version="1.0" encoding="UTF-8"?>
<rKmDocument>
  :
  <Title><![CDATA[document_title]]></Title>
  <ExternalDocumentName>
    <![CDATA[document_filename]]>
  </ExternalDocumentName>
  :
</rKmDocument>
```

This is an example of an .xml document with metadata:

A file named `5342.xml` placed in the Troubleshooting folder that contains metadata for the `readme.patch.txt` file. It contains these elements:

```

<?xml version="1.0" encoding="UTF-8"?>
<rKmDocument>
  <Title>
    <![CDATA[Readme Patch]]>
  </Title>
  <ExternalDocumentName>
    <![CDATA[readme.patch.txt]]>
  </ExternalDocumentName>
  <Summary>
    <![CDATA[Prior to installing this patch, ensure that...]]>
  </Summary>
  :
</rKmDocument>

```

.XML 'authored' documents

All .xml authored documents (3) have an .xml file extension and contain these elements at a minimum:

```

<?xml version="1.0" encoding="UTF-8"?>
<rKmDocument>
  :
  <Title><![CDATA[document_title]]></Title>
  <DocType><![CDATA[document_type]]></DocType>
  :
</rKmDocument>

```

This is an example of an .xml authored document:

A file named `AuthLicense.xml` placed in the *Troubleshooting/RTF Authoring* folder that is a Problem/Solution (probsol) document type. It contains these elements:

```

<?xml version="1.0" encoding="UTF-8"?>
<rKmDocument>
  <DocType>
    <![CDATA[probsol]]>
  </DocType>
  <Title>
    <![CDATA[A licensing error appears when authoring RTF documents]]>
  </Title>
  <Summary>
    <![CDATA[The "localhost" URL does not support licensing.]]>
  </Summary>
  <CreationDate>

```

```

        <![CDATA[07/21/2003 11:45:37]]>
    </CreationDate>
    <rtf_field1 xml:space="preserve">
        <![CDATA[<p>A licensing problem is encountered when the user tries to
            Author rich-text-field documents.</p>]]>
    </rtf_field1>
    <rtf_field2 xml:space="preserve">
    <![CDATA[<p>
        1.When logging into the application server, use the server name (for example,
        http://servername/oa/login.jsp) instead of http://localhost/oa/login.jsp.
        <br />
        2.As the Admin user, check the Server URL setting under the Common tab in
        Administration Settings to ensure that the server name for the Get-Answers
        server is correct.
        <br />
        3.Examine the DNS mappings on your system and ensure that each server
        name is correct.
        </p>]]>
    </rtf_field2>
</rKmDocument>

```

Creating XML export files

You must convert structured documents from other knowledgebase applications such as Tivoli Service Desk to an XML format that Get-Answers can read. This section describes the format your XML documents must use.

The <DocType> attribute in the XML exported from KBMigrate (and any manually created by the user) is imported as a lower case StorageValue in the DocType.

For Example:

```
<DocType>Reference</DocType>
```

is mapped to a DocType with a Name of Reference and a StorageValue of reference . It maps directly to the out-of-box Get-Answers Reference DocType. Users should be aware that Knowlix migrated documents have a Reference DocType but do not use the same form fields as the Get-Answers Reference DocType. This means you should either re-personalize the out-of-box Reference Type (if they have no existing documents in the system of this type), or you should modify the XML used by the Document Import to change the <DocType> element to a unique (case-insensitive) DocType.

Creating the XML documents

Each field in the XML document contains data. The following table describes the supported fields. After you import the documents, the fields reside in the database. Defined fields such as Title are discrete and use a field in the database. However, you can use any fields you like in your XML documents. Fields in your documents that are not listed below are written to an XML metadata file, which is then stored in the database as a binary large object (BLOB) field.

When creating fields different from the fields in the following table, keep the following guidelines in mind:

- Use letters, digits, underline characters, dash characters or periods in your field names. Get-Answers supports them.
- Do not use spaces in the field names.
- See the W3C document “Extensible Markup Language (XML) 1.0 (Second Edition)” at the <http://www.w3c.org/TR/REC-xml> for a thorough list of guidelines on creating XML documents.

The following table shows the fields (XML) that are stored in the database. The Search engine indexes these fields. When you use these fields in your XML export documents, keep the following in mind:

- You must spell these tags exactly as they appear here.
- These tags are case-sensitive. When you use these tags, match the case as it appears here.
- The table includes four Tivoli Service Desk fields: System, Component, Item, and Method (SCIM). Although Get-Answers does not save these fields in a hierarchy, the Search engine does search them individually.
- Wrap each text field with: `<![CDATA[text]]>`
- The fields that are required have “required” in the Field/XML Tag column.

Field/XML Tag	Description	Max Number of Bytes
Component	Tivoli Service Desk Component field	40
CreationDate	Date the document was created. The date format is: mm/dd/yyyy. The default is the current date.	N/A

Field/XML Tag	Description	Max Number of Bytes
DocType	The storage value of the document type. It is a value with no spaces in it such as probsol, errormsg, howto, reference, or any company-specific document type storage value. For an example of how storage value is used, see <i>To create a new document view</i> : on page 317.	32
dtLastModify	Date the document was last changed in any way. The format is mm/dd/yyyy. The default is the current date.	N/A
ExpDate	Date the document expires and should be reviewed. This field is used only for reporting. The format is mm/dd/yyyy. The default value is last modified date plus one year. (Last modified date appears as LastModified in the database.) If no last modified date is specified, the ExpirationDate field default is then CreationDate plus one year. If no creation date is specified, the default is the current date plus one year.	N/A
ExternalDocument Name	The file name of the externally created document (pdf, doc,etc.) that resides in the same folder as this xml file. This is required for xml documents with metadata for externally created documents.	N/A
guid	Global document ID that identifies the document within the system from which the document is imported. Do no use spaces or blank characters in this field.	38
Item	Tivoli Service Desk Item field	40
OwnedDocs	Semicolon-delimited list of any files associated with this document's team. This includes images, word processing documents, executables, and so on.	N/A
Summary	The summary of the document or synonyms that help the user find the document. You cannot use unmatched single quotes, apostrophes, or unmatched double quotes here.	1024
System	Tivoli Service Desk System field	40
Title (required)	Document title or subject	128

This is an example of a company-generated .xml authored document:

```
<?xml version="1.0" encoding="UTF-8" ?>
- <rKmDocument>
  - <DocType>
    <![CDATA[ ProblemSolution ]]>
```

```

</DocType>
- <LegacyId>
  <![CDATA[ 50541D2078FE910E7C_0202 ]]>
</LegacyId>
- <Group>
  <![CDATA[ Approval_Initial ]]>
</Group>
- <Title>
  <![CDATA[ Rich Text example with all rich text markup from Knowlix ]]>
</Title>
- <Product_Class>
  - <![CDATA[ ]]>
</Product_Class>
- <Operating_System>
  - <![CDATA[ ]]>
</Operating_System>
- <Creation_Date>
  - <![CDATA[ 08/26/2003 11:51:36 ]]>
</Creation_Date>
- <Last_Modified>
  - <![CDATA[ 08/26/2003 11:58:43 ]]>
</Last_Modified>
- <Priority>
  - <![CDATA[ 0 ]]>
</Priority>
- <Problem renderHTML="true" xml:space="preserve">
  - <![CDATA[
    <p align="left"></p>
    <p align="left"></p>

]]>
</Problem>
- <Solution renderHTML="true" xml:space="preserve">
  - <![CDATA[
    <p align="left">This is a line of regular text</p>
    <p align="left">This is <b>bold</b></p>
    <p align="left">This is <i>italics</i></p>
    <p align="left">This is <u>underlined</u></p>
    <p align="left"></p>
    <p align="left">This is <b><i>bold and italics</i></b></p>
    <p align="left"></p>
    <p align="left">This is <b><u>bold and underlined</u></b></p>
    <p align="left"></p>
    <p align="left">This is <b><i><u>bold and italics
      and underlined</u></i></b></p>
    <p align="left"></p>
    <p align="left">This is <i><u>italics and underlined</u></i></p>
    <p align="left"></p>

```



```

- <![CDATA[ ]]>
</OwnedDocs>
</rKmDocument>

```

Changing field size in the database

If you want to increase (or decrease) the size of a field in the database, you can do this using the KmDocument.tbl file and rKmDocument.xml file.

To change the field size in the database:

- 1 Open the KmDocument.tbl file, which you can find in the following directory:
\WEB-INF\bizdoc\tables
- 2 Find the field whose size you want to change. Here is an example of the field “Title.”

```

<Field name="Title">
  <Type>STRING</Type>
  <Length>128</Length>
  <MappingType>DIRECTFIELD</MappingType>
  <SqlName>Title</SqlName>
  <DefaultValue/>
</Field>

```

- 3 Change the number of characters in the <Length> line. Change 128 to 162, for example.
- 4 Save the file.
- 5 Open the file, rKmDocument.xml in \WEB-INF\apps\oaagen\schema and locate the field.
- 6 Change the *length* = “*x*” attribute to the new length.
- 7 Save the file.

Adding fields for search engine indexing (import)

The import process generates the FIELD definitions for you and saves them in an rware_cfg.txt file in the same folder as the KmDocument.xml file. This folder is:

```

\WEB-INF\apps\oaagen\schema\extensions\

```

Once you run the import process to add fields to the `KmDocument.xml` and `rKmDocument.xml` files, use the procedure described in this section to make sure the Search engine finds them during searching.

To add fields for indexing:

- 1 Backup the `rware.cfg` file in the `<search-engine-install-path>\Peregrine\config` directory on your search engine server.
- 2 Open the file `rware.cfg`.
- 3 Find the LIBRARY “KMLib” section of the file.
- 4 Paste the contents of `rware_cfg.txt` into the KMLib section of the `rware.cfg` file.
- 5 Save the file.

Adding fields for search engine indexing

You can also add a field for search engine indexing without using the import process.

- 1 Backup the `reware.cfg` file in the `<search-engine-install-path>\Peregrine\config` directory on your search engine server.
- 2 Open the file `rware.cfg`.
- 3 Find the LIBRARY “KMLib” section of the file.
- 4 For each field you added to the XML schemas, add the following text to the LIBRARY KMLib section, substituting “Question” with the name of your field and “113” with the size of your field:

```
FIELD "Question" {
    INFO "Question";
    UF_NAME "Question";
    PRECEDENCE 1;
    SIZE 113;
    TYPE STRING;
    FLAGS STORED INDEXED VISIBLE NATURAL_LANGUAGE USER_SEARCH
    WITH_BODY SORTABLE SEARCHABLE RESULTS_LIST DOC_VIEW;
}
```

In sum, change the information in the FIELD, INFO, and UF_NAME fields, and enter the size in bytes in the SIZE field. The type is always STRING.

5 Save the file.

Note: See *Changing field size in the database* on page 298 to update the field size in the database for the field you added.

Converting Knowlix data

To convert Knowlix data, use Peregrine's conversion utility to format your documents and create the required folder structure for Get-Answers. If you have purchased a license to upgrade from Knowlix to Get-Answers, then you have this application. You can use it now and then go to the next section when you are ready to import your data to Get-Answers.

If you do not have the conversion utility and would like to purchase it, contact your Peregrine Professional Services representative.

Preparing for the conversion from Knowlix

The following are the steps you should perform to prepare the documents you are planning on converting from Knowlix to Get-Answers.

- 1 Move all knowledge articles from Unofficial.nfo to the correct category
- 2 Move articles into separate nfos according to their main category. Categorization of documents is simplest while importing into Get-Answers.
- 3 For each knowledge article type you can use KnowlixAuthor to:

Note: You should use print screen to capture and save the information you will need when to prepare to migrate documents and manage the documents after they have been migrated.

- a See the list of knowledge article types.

To see the list of knowledge article type that you use, from KnowlixAuthor, create a new article (Edit/New Entry).

View the list of document types in the document type drop-down box.

- b View the input forms used.

To capture an input form, from KnowlixAuthor, open each form in form designer.

View each field, including the actual name used, which are imported into Get-Answers.

Note: The field name imported into Get-Answers will have spaces replaced with underscores (_) because xml standards do not allow for spaces in field names.

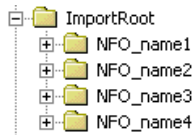
- c View the document views used.

While you are viewing each document type (in KnowlixAuthor), print it as well to the view used for each document type. All of this information will be useful later when you are creating new input forms, edit forms, views for the documents in Get-Answers.

Running the migration from Knowlix

These are the recommended procedures for using the Knowlix migration wizard to import knowlix data to Get-Answers. See the Knowlix migration document for more information.

- 1 Run the Knowlix migration wizard on each nfo.
- 2 When you make each category of knowledge documents (Human Resources for example) a separate nfo in Knowlix, the migration wizard generates a directory with the same name as the nfo. If you want the nfo name to be the name of the top-level category in Get-Answers, put this directory under ImportRoot. The name of this directory becomes the name of a top-level category in Get-Answers.



Importing your data to Get-Answers

Once you have converted your data, either from Knowlix or from another application, such as Tivoli ServiceDesk, use the procedure in this section to import the data into the Get-Answers database.

To import converted documents into Get-Answers:

- 1 Move the data you have converted to a directory on the Get-Answers server:
- 2 Start Get-Answers.
- 3 Click the **Get-Answers** tab.
- 4 On the left panel, click the **Import Documents** link.

The Import Document page opens, as shown here.

Path on the application server where documents to be imported reside:

Category Defaults

Document Ownership Team for New Categories:

External Document Options

Requiring XML Metadata Files allows for both External and Authored documents to be imported in the same batch. When used with External documents it allows custom metadata to be specified for each document. Direct Import assumes that ALL documents in this batch are External Documents. This means that any file (including XML) encountered by the import process will be imported as an External document.

Require XML Metadata Files
 Direct Import

ExpirationDate (for reporting purposes)

Enter the number of months after Create Date or Last Modified Date when the document content expires

Create Date
 Last Modified Date

Note that Create Date and Last Modified Date default to today if not specified.

- 5 On this page:
 - Type the directory path for the location of the documents you are importing. (Required entry)
 - In the Document Ownership Team field, choose a document team to manage the documents.
 - In External Document Options select either Require XML Metadata Files (allows you to import files containing both External and Authored documents with custom metadata), or Direct Import (all the documents being imported are External documents).
 - In the Expiration Date section, choose the number of months before the documents expire, and then choose whether the documents expire by creation date or last modified date.

6 Click Import.

The following message appears: “The file import is complete. See the `getanswers_document_import.log` for detailed results.”

Managing migrated documents

After documents are migrated from Knowlix, you need to manage these documents by performing the following tasks:

- Setup permissions
- Setup searching
- Extend the database
- Create input and edit forms
- Create views
- Remove like-named document types

Setting up permissions

The sample user login “suser,” by default, has permission to create the categories, import the documents, create document views, personalize input forms, and personalize edit forms (also known as Workflows).

Note: Permission to create categories and to create document views requires Team Owner permissions in the document teams. Permission to import documents requires Get-Answers Administrator permissions, which are set in Set Security Capabilities. Permission to personalize input forms and personalize edit forms (Workflows) requires Personalization System Maintenance permissions, which are set in Set Security Capabilities.

You may want to give every owner the permission to administer the personalization of forms. Unfortunately, there is not way to prevent one document team owner from overwriting the changes that another document team owner made which have a system-wide effect.

Use the Set Owners Permission page to view and update document ownership team permissions.

Get-Answers tab > Manage Document Ownership Team link > Search > select Document Team > Set Owner Permissions

Click Add User or Add Role to assign Owner permissions. An owner permission is required.

Owner Permissions:	
Name:	Get-Answers Team

Owner Permissions by Role	
Remove	Roles

[Add Role](#)

Owner Permissions by User	
Remove	Users
Remove	user, super
Remove	Owner, Otto

[Add User](#)

[Save](#)

Use the Set Security Capabilities page to update the security capabilities.

People > Search > Admin > Person Details > Set Security Capabilities

Please select from the list of available security elements.

Select	Capability	Description
<input type="checkbox"/>	Assets Management	Manage Assets
<input type="checkbox"/>	Assets Setup	Manage Assets Setup Details
<input checked="" type="checkbox"/>	People	Manage People
<input type="checkbox"/>	Organizations	Manage Organizations
<input checked="" type="checkbox"/>	Assign Role	Assign Roles to people
<input checked="" type="checkbox"/>	People Setup	Manage People Setup Details
<input type="checkbox"/>	Places	Manage Places
<input type="checkbox"/>	Places Setup	Manage Places Setup Details
<input checked="" type="checkbox"/>	System Maintenance user	Full access to system maintenance and administration activities.
<input checked="" type="checkbox"/>	Portal	Allow access to the Peregrine Portal
<input checked="" type="checkbox"/>	Personalization System Maintenance	Access to the system maintenance and administrative functions
<input checked="" type="checkbox"/>	Personalization default	Default capabilities for a Standard User
<input type="checkbox"/>	Get-Answers Administrator	View all Get-Answers Document Ownership Teams.
<input checked="" type="checkbox"/>	Get-Answers Reports	View all Get-Answers Reports.
<input checked="" type="checkbox"/>	Notification Services Administrator	Notification Services Administrator.
<input checked="" type="checkbox"/>	Notification Services GUI	Allow a user to view the Notification Services GUI.
<input checked="" type="checkbox"/>	Update Preferences	Allow a user to view and update their work schedule and device preferences in Notificat
<input checked="" type="checkbox"/>	Send Notifications	Allow a user to view the Send Notification activity in Notification Services.
<input checked="" type="checkbox"/>	View Notifications	Allow a user to view the Inbox and Outbox activities in Notification Services.
<input checked="" type="checkbox"/>	Workflow administrator	access to admin interface
<input checked="" type="checkbox"/>	Workflow Template designer	access to the designer interface
<input checked="" type="checkbox"/>	Workflow Process	add rights to edit a running process
<input type="checkbox"/>	Workflow Request	access to the request module
<input checked="" type="checkbox"/>	Workflow Standard User	basic access to the task list

Using the extended fields in searching

Copy the text from the `rware_cfg.txt` file to the `rware.cfg` file, following these rules:

- Remove the duplicates.
- Keep the largest of the duplicates if you want the entire field to be searched on.
- Remove fields that you do not want searched on. For example, if you do not want the document's history fields searched, you can remove it from the `rware.cfg`).

Extending the database

The database is automatically extended during imports or migrations; however, you have to restart the application server for the extensions to the schema to be enabled. (See *Creating schema extensions* on page 312.) The search engine must also be restarted (to make use of the new search fields). The search engine needs to re-index all documents to include the newly imported documents.

Creating input and edit forms

When you migrated the Knowlix documents to Get-Answers, the system created document types for these documents. In order to make these new document types useful for contributing new documents to the system or editing documents that you migrated, you need to create an input form and an edit form for each document type.

Note: See *Chapter 12, Document Types and Views* and *Chapter 5, Personalization* for additional information.

To create a new input form and edit form:

- 1 From the Get-Answers tab, click the **Contribute New Document** link.
- 2 Select the document type.

The Create New Document page opens.

Please fill in the requested information and click the submit button.

Entry Form

Title:

Document Type: Reference

Summary:

Document Ownership Team: Get-Answers Team

Expiration Date: Aug 5 2004

See Details

Add Content Choices

Link to Other Doc Weblink New Upload Image Shared Content

Standard | [Default] | Normal | Normal

WYSIWYG Source View

edit-on® Pro by RealObjects

Submit Document Preview Document Go Back

Personalization icon

This page probably does not have the fields that authors may need.

- 3 Add those fields by selecting the personalization icon (a wrench) to open a personalization window that lists all the fields you can add to your input form.

Use the information gathered from KnowlixAuthor (*Preparing for the conversion from Knowlix* on page 301) to determine which fields you want document authors to see. See *Chapter 5, Personalization* for more details on personalizations.

- 4 Click Save when you complete personalization.

The Create New Document page opens with the new personalization added.

Now use this form with the personalization changes you made to create a sample document.

Note: You must complete the Document Ownership Team and Document Type fields.

- 5 Click Submit.

The document you submitted goes into the workflow (Triage) where you can open it for editing.

- 6 In Workflow, open and accept the triage workflow assignment associated with the sample document that you submitted.

You can use the same steps to create the edit form that you used to create the input form. You do not need to use the same fields, or all of the fields that you used in authoring the document, although they are all available. You have to use the Document Ownership Team and the Document Type fields.

Note: Some fields are populated automatically, such as date the document was created.

- 7 On most edit forms, you may want to change some of the fields from read only to allow input or make some entries required. For a detailed explanation of these procedures, see in *Chapter 5, Personalization, Configuring field attributes*.
- 8 When you complete all the personalization changes, click **Save** in the Personalization Document Detail window.

You should now have a personalized edit form saved, so you can delete the sample document you have been using to create the edit form.

The next time you open a document of this type for editing, the document will use all of the personalization changes you made when you created the edit form.

Creating views

You must create a document view so that the documents using that view can be displayed.

To create document views:

- 1 Click **Manage Document Types**.
- 2 Select the document for which you want to add a view.

3 Click the Add link next Document Views.

Please fill in the requested information and click the submit button.

4 Use the field names in the field list to add them to the view.

See *Chapter 12, Document Types and Views* for adding fields to the document view.

5 Click Add View to save the new view.

Removing like-named document types

You should remove the sample doc types supplied with Get-Answers including Error Message Cause, How To, Problem Solution, and Reference document types if you have like named document types from Knowlix.

If users start submitting documents with the sample versions, you will have document type management problems from duplicate types, requiring you to support two versions of every document view, every input form, and every edit form for the document types.

See *Chapter 12, Document Types and Views* for information about deleting document types.

Creating schema extensions

Schemas are XML documents that modify the data in the database. Schemas describe the structure of the data and the relationships between the data in the database. The Get-Answers import process provides schema extension files for your data during the import process. These schema extensions are saved in the KmDocument.xml file in the following directory, which you can find in this directory:

```
\WEB-INF\apps\oaagen\schema\extensions\
```

The schema extension generated by the Import Documents activity defaults the field labels to the name of the field. These are not localized. You have to add \$\$IDS mappings in the schema and string files to localize them.

To localize the label of a new field:

- 1 Open the rKmDocument.xml file in this directory:

```
\webapps\oaa\WEB-INF\apps\oaagen\schema\extensions\
```
- 2 Find the line that begins with <attribute name= , e.g. <attribute name="OperatingSystem" label="OperatingSystem" type="string" />
- 3 Change the label="OperatingSystem" to

```
label="$$IDS(Entities,Entities_OperatingSystem_Label)"
```
- 4 Open the Entities_en.str file in this directory:

```
\webapps\oaa\WEB-INF\apps\oaagen\
```
- 5 Add this line alphabetically so it is easily found afterwards.

```
Entities_OperatingSystem_Label, "Operating System"
```
- 6 For each language in the \webapps\oaa\WEB-INF\apps\oaagen\ directory or in a directory below it, add the attribute's label for that language.
 For example, in the Entities_de.str file, add this line for the German string:

```
Entities_OperatingSystem_Label, "Betriebssystem"
```
- 7 Repeat this procedure for each field you added.

Using schema extensions to manually add new fields

If you are not using the import process and need schema extensions follow the procedures described in this section.

You can add as many new fields as you want by repeating one line and changing the properties of that line, which these procedure describes how to do. In the first procedure, you change the logical mappings of the fields. In the second procedure, you change the physical mappings.

Note: Do not use this procedure if you are migrating Knowlix data. See the section *Converting Knowlix data* on page 301 for more information on Knowlix migration.

To change the logical mappings in the Get-Answers schema extension file:

- 1 The schema extensions are saved in the KmDocument.xml file in this director:

```
\WEB-INF\apps\oaagen\schema\extensions\
```

- 2 Find the line that begins with `<attribute name=.`

This example shows what the KmDocument.xml schema extension file looks like before you change it. The attribute name line appears in bold text for this example only.

```
<schema>
  <documents name="base">
    <document UniqueField="" extends="" name="rKmDocument"
label="$$IDS(Entities,Entities_KmDocument_Label)"
preexplorer="preexplorer.rKmDocument.kmDocumentPreexplorer"
loadscript="loadscript.rKmDocument.kmDocumentLoadScript">
      <attribute name="OperatingSystem" label="Operating System" type="string" />
    </document>
  </documents>
</schema>
```

- 3 Copy the line that begins with `<attribute name=` and paste it below the line.
- 4 In the line you pasted, change the value in quotes to the field you want to add. For example, change “operating system” to “job title”.
- 5 Repeat steps 3 and 4 for each field you want to add.
- 6 Save the file.

To change the physical mappings:

- 1 Open the rKmDocument.xml file in the following directory:

```
\WEB-INF\apps\oaagen\extensions\rome\
```

- 2 Find the line that begins with `<attribute.`

This example shows what the rKmDocument.xml document looks like.

```

<schema>
  <documents name="rome">
    <document CallableClass="" CacheType="DEFAULT" string="Title"
table="KMDOCUMENT" ejb="KmDocument" name="rKmDocument">
      <attribute callmethod="" length="42" field="_null"
        member="OperatingSystem" name="OperatingSystem" />
    </document>
  </documents>
</schema>

```

- 3 For each field that you added in the KmDocument.xml (physical mappings) document, copy and paste the <attribute line.
- 4 Change this text in the attribute line you have pasted.
 - Change the length= to your preferred length for the field. For example, change length="42" to length="56".
 - Change the member= to match the name of the field. For example change, member="OperatingSystem" to member="JobTitle".
 - Change the name= field to match as well. For example, change name="OperatingSystem" to name="JobTitle".

Important: For each field you added in the KmDocument.xml schema, make sure you change each of these fields in the rKmDocument.xml schema.

- 5 Save the file.
- 6 If you need to localize the labels for the new fields, see *To localize the label of a new field:* on page 312.

12 Document Types and Views

CHAPTER

This chapter describes how to work with Document Types and Document Views. The topics covered in this chapter are:

- *Document Types* on page 315
- *Document Views* on page 316
- *Using document types to manage documents* on page 316

Document Types

Document types are templates for documents in Get-Answers. For example, you create a Document Type called Payroll Error. When there is an error in processing payroll, you want your staff to use the Payroll Error form to write up the problem. In the Payroll Error document type, you add a field called “Error.” You want users to describe the error in this field. Then you add a field called “Problem,” in which you want users to describe the underlying problem that caused the error. Finally, you create a field called “Solution.” Here users add their solution to the problem.

Get-Answers includes several default Document Types. These include How-To, Problem-Solution, and External. These default Document Types provide the basic structure for Document Types that you create. If you later delete your customized Document Types, the default Document Types retain their basic features.

You should use the External Document Type as a template when you need to create a new Document Type not included in default Document Types. Because the External Document Type is intended as a template for other Document Types, it cannot be modified.

Document Views

The Document Views function has two purposes:

- To provide users a way to customize how their information looks in each form.
- To provide a way for administrators to allow users to see only information that their role and permissions allow them to see. This way, users with different permissions can see the same documents, but only those users with certain permissions see sensitive information.

Using document types to manage documents

This section describes how to manage the documents in your documentation library by effectively using documentation types, input forms, views, and roles. You can add new views to existing document types and then control the access to these views with the role attribute. You can also add new document types to the standard document types provided by the system.

The tasks explained in the section are:

- Adding a view for an existing document type
- Adding a role to a view
- Adding a new document type
- Adding a new input form for a document type

Important: You can add document types for users. These forms are templates for users. Users make copies of the document types. For example, a user who uses the document Error Message/Cause is using a *copy* of the document type Error Message/Cause to record information. When you add document types, you must personalize (customize) them in three places before they can run in Get-Answers. You must personalize the Authoring, Workflow and Preview aspects of the document type. This section explains how to add and personalize new document types. To add document types, you must log in with a user id that has both Admin and Owner rights so you can access all modules required in this procedure.

Adding a view to a document type

You can add a document view to an existing document type to include more information about the document or to limit the amount of information that a user may have to provide when adding a new document. Whenever you create a new document view, you must also select the role or roles allowed to use the new view.

To create a new document view:

- 1 Log in to Get-Answers.
- 2 From the Peregrine Portal, click Get-Answers tab.
- 3 In the Activity menu, click **Manage Document Types**.

A list of document types appears.

Please click on any item to view it in detail.

Name	Description
Problem/Solution	Description of a solution for a problem.
External	A document created outside of Get-Answers. Examples are MS Office Documents, PDF, HTML, etc.
How-To	Question and Answer fields you can edit
Reference	A one-field description of the reference.
Error Message/Cause	Description of an error message, steps taken before receiving the error message, and a work-around.
Test Case	This is sample document type for QA

- 4 Click document type you are adding a view to.

The Document Type Details window opens.

Click Add to open the Document Type window.

- 5 Enter a name for the view, for example, Test Case.
- 6 Continuing with the example, enter testcase in Storage Value as one word with no spaces. Storage Value is the external representation for the particular string name (the view name) you are creating.
- 7 Enter a description of the example, such as, “This is a sample document type for QA.”
- 8 Next to Document Views, click **Add**.

The Create New Document View page opens with Document View Details section, the Toolbar and Editor, and Add Content Choices sections available so that you can now begin adding the content for your new view.

Please fill in the requested information and click the submit button.

RTF editor window

- 9 Enter a name for the view, for example “Default Test Case.”
- 10 Set the Security Level. Zero (0) is the highest security and 0 is reserved for the most secure view. In this example, use 10 because this a default view which will be for everyone.
- 11 To insert a field in the view, position your cursor in the edit window (RTF editor window) to where you want the field to appear on the form and select the field name from the Fields List drop-down list. Click **Insert Selected At Cursor**.

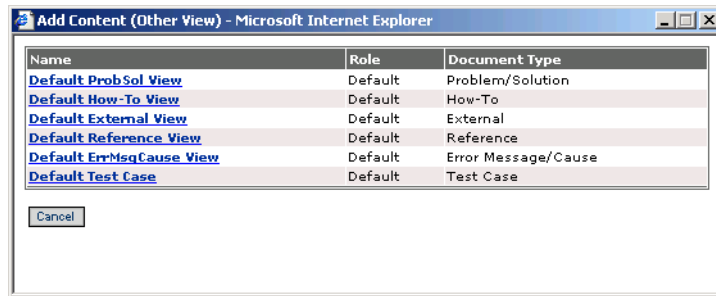
This is a list of standard fields available.

Field Name	Description
Author	The person responsible for the content and maintenance of the document; usually a Document Team Owner.
Author Name	The person who originally submitted the (legacy) document; a string of characters and not a reference to a person in the database.
Checked Out By	Not presently used; available for customer use.
Component	A carryover from Tivoli Service Desk; available for customer use.
Creation Date	The date that document was added to the system, e.g., 2003-5-11.
Date Document Last Modified	Not used.
Document Ownership Team	The team that owns this document.
Document Type	Type of document such as 'How to'; associated with a document ownership team and with a set of views to format the document content.
Expiration Date	Type of document such as 'How to'; associated with a document ownership team and with a set of views to format the document content.
Expiration Date	The date that document is considered out-of-date; used for reporting purposes; generally one year after doc was added to the system, e.g., 2004-9-19.
File Name	The name of physical file.

File Size	The size of file in bytes, usually displayed in KB or MB.
Flex0 to Flex24	These are 50-character string fields in the database that are configurable by the customer.
FlexDate0 to FlexDate4	These are datetime fields in the database that are configurable by the customer.
Item	A carryover from Tivoli Service Desk; available for customer use.
Last Modified Date	The date that the document or metadata was last changed, e.g., 2003-9-19.
Legacy ID	The Id / Identification number of the document in the legacy system.
Locale	The regional language associated with the document, e.g., French, German, etc.
Method	A carryover from Tivoli Service Desk; available for customer use.
Published	Published status of the document, either 'Published' or 'WorkingCopy.'
Published Document	If this is the working copy version of a published document, the id of the published document, otherwise zero.
RTF 1 to RTF 5	These are the rich-text fields in the document. RTF 1 is the topmost and RTF 2 is the second, etc.
Select 1 to Select 5	These are customer-configurable sets of values that are used in up to 5 drop-down boxes.
Summary	Up to 1024 characters that describe the document contents.
System	A carryover from Tivoli Service Desk; available for customer use.
Title	The title of the document (up to 128 characters).
Usage	A numeric value that is incremented when a document receives a 'Useful' rating and decremented for a 'not useful' rating.
Unique ID	This is generated by Get-Answers and used internally.
Unique Identifier	This is generated by OAA Bizdoc and used internally.

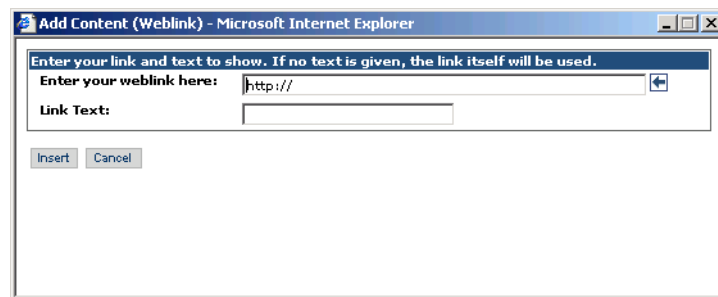
- 12 You can use the formatting features of the editing tool to format the appearance of the field label and position in the form. See the *Get-Answers 4-1 User's Guide* for more information about the edit-on Pro features for formatting text.
- 13 Continue adding fields on form using Field List drop-down and Insert Selected At Cursor.
- 14 You can also use the buttons in Add Content Choices to add additional content to the new document view. The buttons are:
 - **From Other View** - use this button to add content from another view. The content is added at the current position of the cursor. This is very useful for modifying an existing document view.

When you click **From Other View**, the Add Content (Other View) window opens.



The view you selected is inserted into the view you are adding.

- **Weblink** - use this button to add a link (href) to another document. When you click **Weblink**, the Add Content (Weblink) opens.

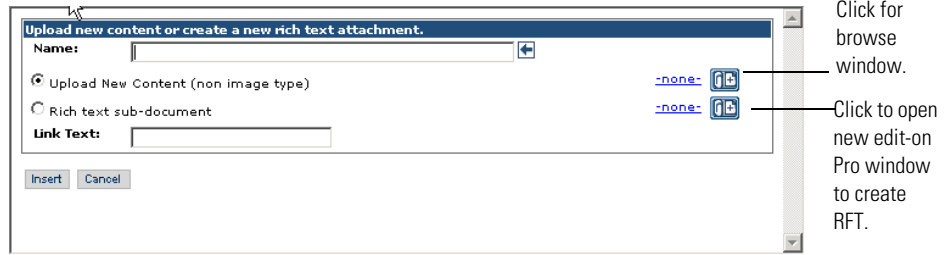


Type the URL for the link, a name for the link, and click **Insert**.

This creates a link in the new view you are adding.

- **New Upload** - use this button to add an external attachment. The attachment is usually a Word document, txt file, PDF file or some other type of external document. Because this document is an attachment, it is not included in the index and does not appear in any search results.

When you click New Upload, the Upload new content window opens.



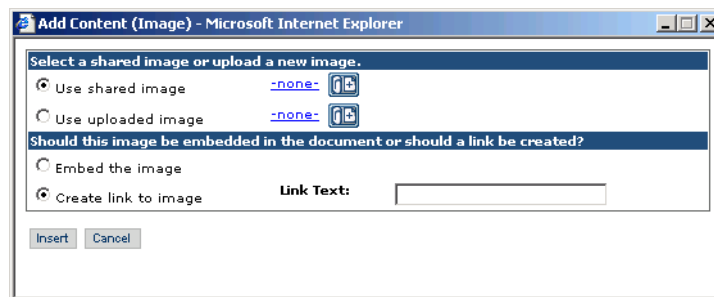
You can create two different types of documents:

a document created externally, which opens a browse window where you can enter the path for the external document (non-image).

or an RTF document, which you create at the time you are doing the upload using the edit-on Pro editor in the pop-up window that appears when you select Rich text subdocument and click the icon on the right.

- **Image** - use this button to add an image to the document view. The image can be either a shared image or embedded in the document. A shared image is one that has already been uploaded and is usually used by more than one document view.

When you click **Image**, the Add Content (Image) window opens.



You select either to use a shared image (one already uploaded) or to upload and image. Click the appropriate icon to open a browse window to specify the path for the location of the image.

You also select either to embed the image in the document view or put a link to the image in the document view.

- **Shared Content** - use this button to add content that has already been uploaded to the database, for example, a PDF file.

When you click **Shared Content**, the Add Content (Shared Content) windows opens so that you can select the content you want to share.

- 15 Click **Add New View** to save your changes and then **Submit Changes**.

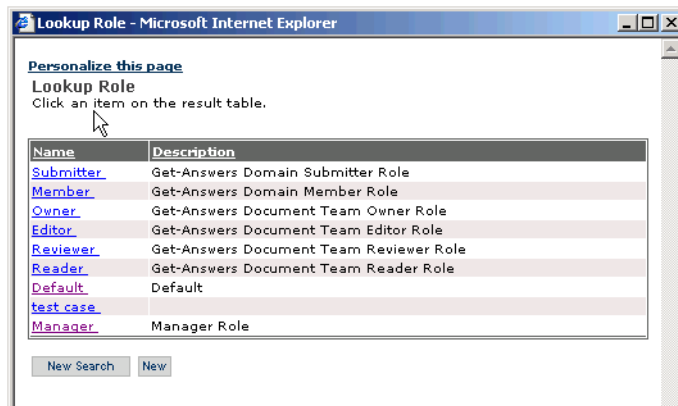
Adding a role to a document view

You next need to associate roles with the view. This allows users who are assigned to the role to use the new document type view you created. This example uses the Default Role (since most all users belong to the Default Role) as an example of how to add a role to a document type view.

To add a role to a document type view:

- 1 From the Get-Answers tab, click **Manage Document Types**.
The Document Type Edit window opens.
- 2 From the list, click the name of the view, for example, Default Test Case View.
The Document View Details window opens.
- 3 Click **Add** next to Roles.
A Roles search window opens.
- 4 Click the search icon (binoculars).
The Lookup Roles window opens.
- 5 Enter the search parameters or just click **Search**.

The Lists of Roles window opens.



- In the list, click the role you are adding to the view.

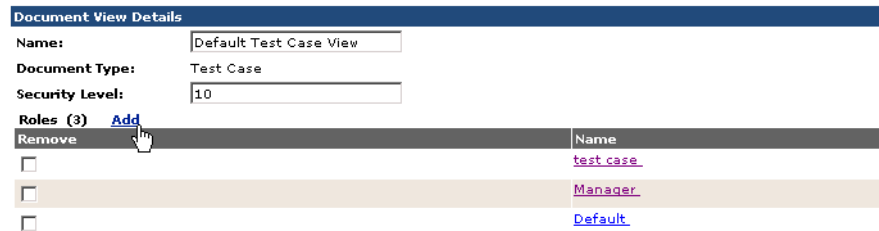
The Roles window opens with the role you selected listed.

- Click OK.

The Document View Details window opens with the role you selected listed in the Roles section.

Please remember to press "Submit Changes" when you are ready to save your changes

View details for this document view and make any needed changes. When finished editing click Save Changes or if no cha



You can use the document view you created to contribute a new document or view documents in the system.

Adding a new document type

Get-Answers comes with a set of default document types, but you can add additional document types using the Get-Answers tab.

To create a new document type:

- Log in to Get-Answers.

- 2 From the Peregrine Portal, click **Get-Answers** tab.
 - 3 Click **Manage Document Types** link.
- A list of document types appears.

Please click on any item to view it in detail.

Name	Description
Problem/Solution	Description of a solution for a problem.
External	A document created outside of Get-Answers. Examples are MS Office Documents, PDF, HTML, etc.
How-To	Question and Answer fields you can edit
Reference	A one-field description of the reference.
Error Message/Cause	Description of an error message, steps taken before receiving the error message, and a work-around.
Test Case	This is sample document type for QA

[New Search](#) [New](#)

- 4 Click **New**.
- The Create Document Type page opens.

Please fill in the requested information and click the submit button.

Create Document Type

Name:

Storage Value:

Description:

Document Views [Add](#)

Remove	Name
[X]	

[Submit](#) [Go Back](#)

- 5 Enter a name for the document type, for example, **Technical Publications**.
- 6 Continuing with the example, enter **technicalpublications** in **Storage Value** as one word with no spaces.
- 7 Enter a description of the example, such as, “This is a sample document type for **Technical Publications**.”

You now need to add a document view to the document type in order for the document type to be useful.

Adding an input and edit form

You must create an input for users (authors) so that they are able to contribute documents of various types. The system comes with a set of document types which are used to contribute a new document, or you can add additional input forms. After you have created a new input form, you can use the form to create an edit form for the document. Documents are created (authored) from the Get-Answers tab and edited from the Workflows tab. When you are creating input and edit forms, you use personalization extensively. You should review and be familiar with the information in *Chapter 5, Personalization* before you begin to create new input and edit forms.

This section explains:

- Using Contribute New Document to create a new input form
- Creating a test document to use to create a new edit form (Workflow)

To create a new input form:

- 1 From the Get-Answers tab, click the **Contribute New Document** link. A list of available document types opens.
- 2 Select a document type to use as a base document for a new input form.

Note: You should select a document type that is most similar to the input form you are creating and has the appropriate roles associated with it.

The Create New Document page opens.

Please fill in the requested information and click the submit button.

Entry Form

Title:

Document Type: Reference

Summary:

Document Ownership Team: Get-Answers Team

Expiration Date: Aug 5 2004

See Details

Add Content Choices

Link to Other Doc | Weblink | New Upload | Image | Shared Content

Standard | [Default] | Normal | Normal | B | I | U | L | H | O | S | A | G | E | F | C | P | M | N | D | E | R | T | I

WYSIWYG | Source View | edit-on® Pro by RealObjects | Insert

Submit Document | Preview Document | Go Back

Personalization icon

This form may not have all the fields that authors need.

- 3 Add the additional fields by selecting the personalization icon (a wrench) to open a personalization window that lists all the fields you can add to your input form. (See *Chapter 5, Personalization* for details.)

Select to add RTF field,

- 4 For example, you may wish to add an edit window for RTF editing using edit-on Pro. You would select RTF1 and move it to Current Configuration.
- 5 Click **Save** when you complete personalization.

The Create New Document page opens with the new personalization added. Now use this form with the personalization changes you made to create a sample document.

To create a sample document using the input form:

- 1 On the form you personalized, type the title of the sample document.
- 2 Enter any additional information required by the form.
- 3 Click **Submit**.

The document you submitted goes into the workflow (Triage) where you can open it for editing.

To create an edit form for the input form:

- 1 From the Workflow tab, select the sample form you submitted from your list of My messages.

The Task Details page opens.

- 2 Click **Accept Group Assignment**.

The Task Details page opens.

Open and accept the triage workflow assignment associated with the sample document that you submitted. You can use the same steps to create the edit form that you used to create the input form. You do not need to use the same fields, or all of the fields that you used in authoring the document, although they are all available. You have to use the Document Ownership Team and the Document Type fields.

Note: Some fields are populated automatically, such as date the document was created.

- 3 On most edit forms, you may want to change some of the fields from read only to allow input or make some entries required. For a detailed explanation of these procedures, see in *Chapter 5, Personalization, Configuring field attributes*.
- 4 Click **Save** to save your personalization changes and close the window.
- 5 Use **Preview Document** to view your changes.
- 6 Use the personalization icon (wrench) to make any additional changes.
- 7 When all the changes are made, select Delete this document from the system.
- 8 Click **Save Changes and Perform Action**.

The system deletes the sample document, but the personalization changes you made for editing documents for this document type remain so that the next time you open a document of this type it will appear in the edit form you created.

Glossary

This glossary contains general terms used when describing Get-Answers, OAA platform, and Workflow.

- Activity** A task or set of tasks that forms one logical step within the process definition. An activity can be a *manual activity* or an *automated activity*.
- Activity instance** A single instance of an activity within a process instance. A process instance can include multiple activity instances.
- An activity that has been started is an activity instance.
- Adapter** Provides a connection between the back-end database and the Web application, allowing data to pass back and forth from the database to the Web browser.
- AND-Join** A point within the workflow where two or more parallel activities are joined and the next logical activity is executed (see *Parallel routing*).
- AND-Split** A point within the workflow where a sequential route splits so that two or more parallel activities are formed for independent, simultaneous processing (see *Parallel routing*). An AND-Join is used to join the parallel activities when their processing is complete.
- Application server** Processes data from a Web application database and delivers it to the Web server.

Archway A Java servlet that listens to HTTP requests from clients and foreign servers, routes the requests to an appropriate server, and returns data or displayable documents. The requests supported by Archway can vary, but they fundamentally consist of queries, data updates, and system events. Archway processes HTTP requests and formats them into messages understood by the Get-Answers processing layer. The resulting messages are ultimately dispatched to a data store adapter which produces an XML formatted result set.

Authoring Authoring is the ability to create new documents and edit the content using an RTF editor.

Audit data An historical record of the progress of process instances and activity instances.

Get-Answers collects the following information for process instances and activity instances:

Process Instance	Activity Instance
Date Started	Date Assigned
Date Ended	Date Due
	Date Ended

Automated activity An activity that is performed by a computer, without user intervention.

Business process A set of linked activities that complete a business objective. A business process is defined in a process definition that can include both automated and manual activities.

Capabilities Capabilities are the tasks that Members, Submitters, Readers, Reviewers, Editors, and Owners can perform. There are seven capabilities including read, create, update, revert, retire, publish, and transfer.

Component template Defines a set of specific activities. A component template can be added to a workflow template.

Deadline A time-based scheduling constraint where the work item for an activity must be completed by a specified time.

categories	Categories contain published documents. Each category is managed by one Ownership Team.
ECMAScript	Server-side scripting language. Used to write scripts for Get-Answers.
Editor	Editor is one of the four Document Ownership Team permissions. An editor has read, create, and update capabilities for any document owned by the Ownership Team. An Editor also has special responsibilities in the editorial workflow.
Editorial workflow	The Get-Answers Editorial Workflow is used to edit and review an unpublished (working copy) document and its metadata.
Escalation	A procedure that is invoked when a specific constraint or condition is not met. An escalation can be automated or manual and generally involves a higher level of authority (see <i>Organization- al Role</i>).
Event	An occurrence that causes the workflow management software to take one or more actions. An event notifies the workflow engine of an internal or external action.
External document	A document created outside of Get-Answers. Examples include MS Office documents, PDF documents, and HTML documents.
HTML	Hypertext Markup Language. A language used to compose Web pages, which can be read and displayed by a Web browser.
HTTP	Hypertext Transfer Protocol. The communications protocol used to connect to Web servers. Sends HTML pages to the Web browser to be read and displayed. HTTPS can be used to provide extra data level security.
Iteration	A repetitive execution of one or more activities until a specified condition is met.
JAAS	Java Authentication and Authorization Service: JAAS is used by Get-Answers to authenticate users. The set of services against which a user must be authenticated can be configured, and each service can be defined as REQUIRED, OPTIONAL, REQUISITE, or SUFFICIENT through login modules.

Java Run-Time Environment	A JRE is required to run Java programs. It consists of the Java Virtual Machine, the Java platform core classes, and supporting files.
JSP	Java Server Page. Allows separation of page content from the design and display of a page. HTML tags with embedded Java source code are executed by the Web or application server. JSP technology is an extension of Java servlet technology.
Manual activity	An activity that requires user resources for performance of the required tasks associated with the activity.
Member	Member is one of the two category permissions. A member has read access to any document published in the category.
Metadata	Metadata consists of information stored about each document, such as file name, title, file size, document type, version number, creation date, and editorial status.
OAA platform	The software platform that the Peregrine Get-It products use. These products are Get-Answers, Get-Resources, and Get-Services. This platform provides features and functionality common to the Get-It employee self-service products. The OAA Platform is a software product included with any or all of the Get-It products and is not sold without them.
OR-Join	A point within the workflow where two or more alternative activity branches are joined into a single activity.
OR-Split	A point within the workflow where a sequential route splits based on a decision upon which branch to take. An OR-Split is conditional and the branch to the next activity is determined by the value returned.
Organizational Role	A group of workflow participants having a specific set of attributes, qualifications, and skills. The participants within the group can perform work items that require a participant who has that set of attributes.
Owner	Owner is one of the four Document Ownership Team permissions. An owner has read, create, update, revert, retire, publish, and transfer capabilities for any document owned by the Ownership Team. An Owner also has special responsibilities in the editorial and triage workflows.

Ownership teams	Ownership Teams manage documents. There are four permissions associated with an Ownership Team. They include Reader, Editor, Owner, and Reviewer.
Parallel routing	A segment of a process instance where two or more activity instances execute in parallel. Parallel routing normally is created with an AND-Split and concludes with an AND-Join.
Peregrine Portal	The first screen displayed when starting a Peregrine Web application. Provides a login screen and access to the modules that make up the application.
Process	A set of process activities designed within the process definition according to the requirements of a business process.
Process definition	<p>A process definition represents a business process and consists of activities where the process tasks are defined.</p> <p>A process definition includes information about the activities and workflow users. Both manual activities and automated activities can be included in the process definition.</p>
Process instance	<p>A single instance of a process as defined by the process definition.</p> <p>A process that has been started is a process instance.</p>
Process role	A mechanism that associates workflow participants with workflow activities. The role defines how the user participates in a specific process or activity.
Process state	<p>A representation of the status of a process instance. The Get-Answers workflow uses the following process states:</p> <ul style="list-style-type: none"> Running—the process instance is running and one or more activities have started. Completed—the process instance has successfully completed all activities. Error—the process instance has encountered an error and stopped.
Reader	Reader is one of the four Document Ownership Team permissions. A reader has read access to any document owned by the team. Readers play no role in the editorial or triage workflows. Readers can author documents.

Reviewer	Reviewer is one of the four Document Ownership Team permissions. A reviewer can read any document owned by the Ownership Team. A Reviewer also has special responsibilities in the editorial workflow.
Roles	Roles consist of a group of users. Permissions are given to roles and/or individual users.
Sequential routing	A segment of a process instance where several activity instances are executed in sequence.
Servlet	A platform-independent Java application component that is used by the system as needed to perform server-side processing (for example, to access a database).
Submitter	Submitter is one of the two category permissions. A submitter has read access to any document published in the category, and can contribute new documents to the category.
Triage workflow	The Get-Answers Triage Workflow is used to examine newly submitted documents that have never been published before, in order to determine if the document should be further reviewed in an Editorial Workflow, published immediately, transferred to a different Document Team, or deleted.
Web application	An application that appears in a Web browser.
Web server	Reads data directly from a Web application or from the application server and converts it to a form that can be displayed by a Web browser.
Work item	The work to be processed by a workflow user, as defined in the associated activity. Work items for a user or group of users are accessed through the worklist.
Workflow	The automation of a business process where tasks are passed from one user to another, as defined by the process definition.

Get-Answers workflow consists of the lifecycle stages of each document. Up to three copies of a document can exist at any time. They include the published copy, the working copy, and the copy currently under revision.

Workflow engine	<p>A software service or “engine” that provides the run time execution environment for a process instance.</p> <p>The workflow engine interprets the process definition, creates process instances and manages their execution, and navigates activities and creates work items for their processing.</p>
Workflow participant	<p>A user that performs the work items assigned through the worklist. Each work item is represented by a workflow activity.</p>
Working copy	<p>Working Copy is a version of the published document in an editorial status.</p>
Worklist	<p>A list of work items associated with a specific user or group of users.</p>
XML	<p>Extensible Markup Language: A documentation meta-language that allows you to author self-describing data documents, which can then be formatted with a style sheet for display in a Web browser or exchanged with foreign systems. Unlike HTML, you create your own XML tags and define their meaning to suit the application.</p>

Index

A

- accessing
 - administration function 260
 - My Requests 282
- activities
 - creating 235, 244, 248
 - definition 329
 - deleting 252
 - End 234
 - Jump activity 249
 - modifying 251
 - notifying by role 239, 241
 - positioning 235–236, 248, 250
 - Sample 234
 - Select 234
 - Start 234
 - task type 237
- activity details
 - Approval activity 245
 - Message tasks 241–242
 - Script activity 242, 243
 - Script tasks 242, 243
 - Task or Approval tasks 238–240
- Activity icon 235
- activity instance
 - definition 329
- activity list 249
- Activity menu 85
- adapter
 - definition 329
 - adapter transactions, viewing 155
- adding
 - component template 249
- Admin module
 - changing Settings 152
 - Control Panel 148
 - displaying message queues 153
 - generating web archive files 156
 - importing and exporting personalizations 155
 - message queues 153
 - script status 153
 - Server Log 150
 - Settings page 150
 - showing queue status 154
 - verifying script status 153
 - viewing adapter transactions 155
- administration function
 - accessing 260
 - monitoring process instances 261
 - starting process instances 264
- Administration of processes page 260
- alarms
 - notification 240
 - types 240
- AND-Join 236
 - definition 329
- AND-Split 236
 - definition 329
- application server
 - definition 329

- Approval task 237
 - activity details 238–240
- Archway
 - definition 330
- Archway architecture
 - building blocks 19
 - clients 21
 - diagram 20
 - document manager 25
 - executing queries against a system 25
 - requests 23
 - XML 21
- AssetCenter 115
- associated applications
 - using with Work Scheduling 13
- audit date
 - definition 330
- authentication
 - overriding the login script 195
 - users 167
- authoring
 - definition 330
- automated activity
 - definition 330

B

- branches 247
- Browse process templates page 265
- business process
 - definition 330

C

- capabilities
 - definition 330
- capability words 41
- changing passwords 160
- changing the Peregrine Portal layout 89
- changing themes 91
- column entries
 - process list 261
- component templates
 - adding 249
 - creating 257
 - list 251
 - saving 259

- Component type 232
- components
 - adding Portal 86
 - creating new 85
- Components icon 250
- Control Panel 148
- Create a New Workflow page 233, 258
- creating
 - component templates 257
 - Jump activity 248
 - new activity 235
 - Select activity 244
 - workflow templates 230–252
- CSS files, editing 99
- customer support 15

D

- deadline
 - definition 330
- deleting
 - activities 252
 - process instances 263
 - workflow templates 255–257
- deploying themes 96
- dictionaries
 - customizing 203
- document manager 25
- document ownership teams
 - managing 55
 - overview 45
- document schema definitions. See schemas
- domains
 - definition 331

E

- ECMAScript
 - definition 331
- editor
 - definition 331
- e-mail
 - notification 239, 240, 241
- Employee Lookup window 239, 241
- End activity 234
- escalation
 - definition 331

- event
 - definition 331
- Event detail page 268
- exporting personalized pages 123, 155

F

- field size 122
- field span 122
- form details 158
- form details, displaying 158
- Form Info, displaying 156
- form information, displaying 92
- framesets, changing 104

G

- getit.admin user rights 146
- group of users
 - managing 32

H

- header graphic, changing 97
- Home page 231, 282
- HTML
 - definition 331
- HTTP
 - definition 331

I

- IBM Websphere portal 156
- icons
 - Activity 235
 - Components 250
 - Jump 248
 - Split 245
 - Trash 252
- icons, personalizing 115
- importing personalized pages 123, 155
- Info button 158
- initiating requests 284
- Integrated Windows Authentication
 - configuring 178
 - security 164
- ISO character encoding. See character encoding
- iteration
 - definition 331

J

- JAAS
 - authentication 167
 - definition 331
 - login modules 168
- Java Run-Time Environment
 - definition 332
- JSP
 - definition 332
- Jump activity 248
 - details 249
 - selecting destination activity 249
- Jump icon 248

L

- labels, personalizing 121
- layers, changing 101
- layout, changing
 - MSIE 89
 - Netscape Navigator 90
- LDAP 164
- Lightweight Directory Access Protocol 164
- lists
 - component templates 251
- local.xml file 146, 151
- log, form details 158
- logging on 282
- logging user sessions 160
- login authentication 167
- login modules, JAAS 168
- login script, overriding 195
- login.asp 187

M

- manual activity
 - definition 332
- member
 - definition 332
- Message activity
 - activity details 241
- Message Details page 241
- message queues 153
- message queues, displaying 153
- Message task 237
 - activity details 241–242

- metadata
 - definition 332
- modifying
 - activities 251
 - workflow templates 253–255
- monitoring
 - process instances 261
- monitoring user sessions 160
- moving personalized pages 123, 155
- My Requests 282

N

- Navigation Menu 231, 260, 282
- Notification Services 239, 241
- notifying
 - by role 239, 241
 - e-mail 239, 240, 241
 - e-mail alarms 240

O

- OAA platform, defined 332
- organizational role
 - definition 332
- OR-Join
 - definition 332
- OR-Split 244
 - definition 332
- overriding the login script 195
- owner
 - definition 332
- ownership teams
 - definition 333

P

- parallel routing 236
 - definition 333
- parameters, defining 152
- password, changing 160
- passwords
 - protecting 164
- Peregrine Portal
 - adding components 86
 - definition 333
 - personalizing 86
- Peregrine Portal, tailoring 95

- Peregrine Systems customer support 15
- Personalization
 - interface, described 113
 - list of standard forms 112
 - settings 117
- personalization
 - adding fields 118
 - arranging field order 119
 - interface description 113
 - requirements 115
 - settings 116
 - user rights 117
- personalized pages
 - moving 123, 155
- personalizing
 - adding a new section to the field layout 119
 - changing field layout 119
 - field size 122
 - field span 122
 - forms 113–122
 - icons 115
 - labels 121
 - portal 86–92
 - read-only field 121
 - required field 122
- personalizing the Peregrine Portal 86
- Portal Components, creating new 85
- positioning activities 235–236, 248, 250
- preXSL, form details 158
- process
 - definition 333
- process definition
 - definition 333
- process instances 231
 - currently running 252
 - definition 333
 - deleting 263
 - monitoring 261
 - process number 267
 - starting 264
 - updating 262
- process list
 - column entries 261
- Process list page 261
- process number 267

- process role
 - definition 333
 - process state
 - definition 333
 - Process submit page 266
 - Process submitted page 267
 - Process type 232
- Q**
- queue status, displaying 154
- R**
- read-only field 121
 - request definition 268
 - request list
 - set up 268
 - requests
 - details 283
 - initiating 284
 - overdue 285
 - changing time zone 285
 - required field 122
 - resetting the server 148
 - reviewer
 - definition 334
 - roles
 - definition 334
 - managing 32
 - overview 31
 - routing
 - parallel routing 236
- S**
- Sample activity 234
 - saving
 - component template 259
 - workflow templates 252
 - schemas
 - defined 126
 - elements 136–??
 - sample 128
 - testing from a URL 24–??
 - uses for extensions 131
 - Script activity 237
 - activity details 242–??, 243–244
 - scripts 242, 243, 244
 - script input, form details 158
 - script output, form details 158
 - script status 153
 - script status, verifying 153
 - scripts
 - testing from a URL 23
 - search engine thesaurus 205
 - Secure Sockets Layer 164
 - security
 - alternate login authentication 195
 - user authentication 167
 - Windows Integrated Authentication 178
 - Select activity 234, 244
 - branches 247
 - details 246
 - example 248
 - scripts 247
 - types 246
 - self-registration 159
 - sequential routing
 - definition 334
 - server log 150
 - ServiceCenter 115
 - servlet
 - definition 334
 - Settings page 152
 - spelling checker
 - customizing 219
 - Split icon 245
 - SSL 164
 - Start activity 234
 - starting
 - process instances 264
 - stop words
 - customizing 200
 - string files
 - translating 107, 108
 - Submitter
 - definition 334
 - support contacts 15
- T**
- tailoring themes 95
 - changing framesets 104

- changing layers 101
 - changing stylesheets 99
 - changing the header graphic 97
 - deploying themes 96
 - Task activity
 - activity details 238–240
 - task types 237
 - Approval 237
 - Message 237
 - Task 237
 - tasks
 - notifying by role 239, 241
 - time-sensitive 240
 - technical support 15
 - template types
 - Component 232
 - Process 232
 - templates
 - component 257–259
 - type 232
 - workflow 230–252
 - themes
 - deploying 96
 - tailoring 95
 - themes, changing 91
 - themes, creating 99
 - time zone, changing for overdue request 285
 - toolbar icons
 - Activity 235, 259
 - Components 234, 258
 - Jump 235, 259
 - Split 234, 258
 - Trash 235, 259
 - Zoom in 235, 259
 - Zoom out 235, 259
 - translating strings 106
 - Trash icon 252
 - types
 - alarms 240
 - selection 246
- U**
- updating
 - process instances 262
 - URL
 - querying scripts and schemas from 23
 - user
 - capabilities 231, 260
 - user registration 159
 - user rights
 - getit.admin 146
 - user rights, Personalization 116
 - user session 158
 - user sessions, logging 160
 - user.log file 160
 - users
 - managing 34
- V**
- viewing
 - overdue requests 285
 - process instances 261
 - request details 283
- W**
- web application
 - definition 334
 - web archive (war) files 156
 - web server
 - definition 334
 - Websphere portal 156
 - windows
 - Employee Lookup 239, 241
 - Workflow 237, 238, 241, 246, 249
 - work items
 - definition 334
 - workflow
 - definition 334
 - designer 230
 - workflow engine
 - definition 335
 - workflow participant
 - definition 335
 - workflow templates
 - creating 230–252
 - definition 230
 - deleting 255–257
 - modifying 253–255
 - saving 252
 - type 232

- Workflow window 237, 238, 241
 - component template list 251
 - Jump activity details 249
 - Select activity details 246
- working copy
 - definition 335
- worklist
 - definition 335

X

- XML
 - definition 335



September 12, 2003