Peregrine Systems, Inc.

Get-Answers 4.2

Administration Guide

Peregrine
SYSTEMS®

Contents

PEREGRINE

About this Guide

Get-Answers is a Web-based, knowledge management application that enables you to capture and store knowledge in a database and then to search for that knowledge when you need it. Using Get-Answers, you can improve the quality and accuracy of the knowledge that people in your company use to do their jobs done and help them to 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 common features and functions to Peregrine products such as Get-Answers, Get-Services, and Get-Resources. You run these products on the 4.2 version of the Peregrine OAA Platform; however, the OAA platform is included with these products and not sold separately from them.

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:

- The Get-Answers Release Notes provide information about new features, corrected issues, and known issues. This document is delivered in print format.
- Get-Answers Installation Guide provides information about installing Get-Answers and the Peregrine® Open Application Architecture (OAA) platform; installing 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 document is delivered in print format.
- Get-Answers User's Guide provides information about searching the Get-Answers document collection, working with documents, authoring new documents, and generating reports. This book is delivered on the Get-Answers CD.
- Notification Services Quick Start Guide explains the concepts, provides step-by-step instructions, and describes the tasks that you can perform using 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 of events.

Typographical conventions

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

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

Special elements

This book uses special elements to help you locate information, as shown in the
following table:

Element	Usage
Important:	Information that is required to complete a task
Note:	Information that is of general interest
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 12, Importing Legacy Data, tells you how to convert data from other applications such as Tivoli ServiceDesk or Knowlix to Get-Answers format.

- Chapter 11, Document Types and Views, tells you how to work with Document Types and Document Views.

Contacting customer support

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

Customer Support

For further information and assistance, contact Peregrine Systems' Customer Support at the Peregrine CenterPoint Web site.

To contact customer support:

1   In a browser, navigate to *http://support.peregrine.com*

2   Log in with your user name and password.

3   Follow the directions on the site to find your answer. The first place to search is the KnowledgeBase, which contains informational articles about all categories of Peregrine products.

4   If the KnowledgeBase does not contain an article that addresses your concerns, you can search for information by product; search discussion forums; and search for product downloads.

Documentation Web site

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

To view the document listing:

1   In a browser, navigate to *http://support.peregrine.com*.

2   Log in with your login user name and password.

3   Click either Documentation or Release Notes at the top of the page.

4   Click the Get-Answers link.

5   Click a product version link to display a list of documents that are available for that version of Get-Answers.

6   Documents may be available in multiple languages. Click the Download button to download the PDF file in the language you prefer.

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

Important: Release Notes for this product are continually updated after each release of the product. Ensure that you have the most current version of the Release Notes.

Education Services Web site

Peregrine Systems offers classroom training anywhere in the world, as well as "at-your-desk" training using the Internet. For a complete listing of Peregrine's training courses, refer to the following web site:

http://www.peregrine.com/education

You can also call Peregrine Education Services at +1 858.794.5009.

CHAPTER 1

Architecture Overview

Peregrine Open Application Architecture (OAA) 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 overview

Peregrine OAA is the underlying architecture for many Peregrine products, including, but not limited to, the Get-It suite of Employee Self-Service products.

OAA Product	Description
AssetCenter Web	Web-based application that enables access to the AssetCenter database to all users without having to install the AssetCenter client.
BI Portal	Web-based reporting tool for creating and executing queries against ServiceCenter 5.1 data; and for generating reports and graphs based on that data.
Get-Answers	Web-based, knowledge management application that enables you to capture and store knowledge in a database, and to search for that knowledge when you need it. Using Get-Answers, you can improve the quality and accuracy of the knowledge that people in your company use to perform their jobs, and help them avoid calls to the service desk.

OAA Product	Description
Get-Resources™	Web-based solution that integrates with AssetCenter Procurement, AssetCenter 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 store them in the ServiceCenter back-end system. This allows users to view tickets from Get-Services and ServiceCenter. Modules include Service Desk and Change Management.

Peregrine OAA 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 Peregrine OAA are monitored and maintained.

The base of Peregrine OAA includes:

Component	Description
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	Peregrine OAA 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.

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

Component	Description
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.

Component	Description
OAA Workflow (Get-Answers only)	Enables workflow capabilities used by some Peregrine OAA 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.

Adapters

The KMAdapter retrieves a hitlist from the search engine using API (application programming interface) calls to the search engine. The API calls are documented in the Convera RetrievalWare SDK (software developer's kit).

The RetrievalWare search engine has a flat file of data for every Get-Answers document that contains the indexable words associated with each document. The flat file also holds the topmost document categories and document ownership team associated with the document. RetrievalWare uses its own database connection (independent of Get-Answers or bizdoc) to read this data from the database. It checks for a changes in any document information every five minutes. The Get-Answers `KMLib` configuration files tell RetrievalWare which document fields to index.

The Web crawler (Spider) is not associated with any relational database. The Get-Answers `KMSpider` configuration files tell RetrievalWare which fields (such as title and top line) to index in the documents that are crawled.

Bizdoc

The rome bizdoc adapter is part of the OAA base code. The KMAdapter uses the rome bizdoc adapter to authenticate the user at login time to determine the user's permissions for a document category or document ownership team .

The Get-Answers Web application also uses the rome bizdoc adapter to insert, update, and delete fields in Get-Answers tables in the relational database.

Peregrine OAA architecture

Peregrine OAA 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 supports Apache Tomcat, WebSphere, and WebLogic.
Common clients	Applications can be deployed with Web browsers (for example, IE, Netscape, and Mozilla), 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:
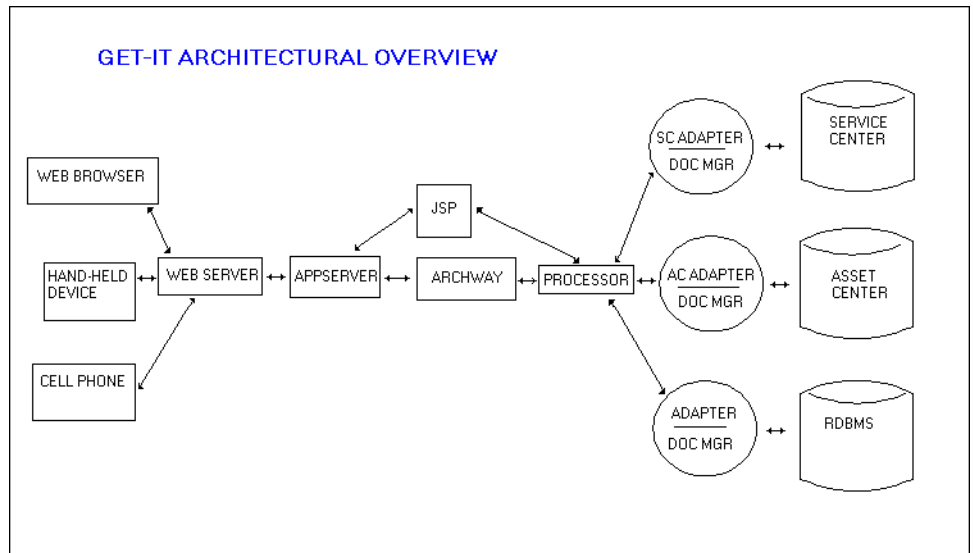
The Archway component listens to HTTP requests from clients, routes the requests to an appropriate server, and returns data or documents. The requests supported by Archway can vary, but they fundamentally consist of queries, data updates, or system events.

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

All requests and responses are formatted using XML, such as the following problem ticket expressed in XML.

```
<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.

OAA scalability

You can ensure that OAA applications perform well as the number of users in your organizations grows. For complete information, see the Guide to OAA architecture and optimization, which is available for download in PDF format in the Employee Self Service section of Product News at *http://support.peregrine.com/support/Get-Answers*.

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/oaa/servlet/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 `/oaa/servlet` mapping assumes that you are using the default URL mapping that Get-Answersautomatically 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/oaa/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 `/oaa/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/oaa/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 `/oaa/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/oaa/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/oaa/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.
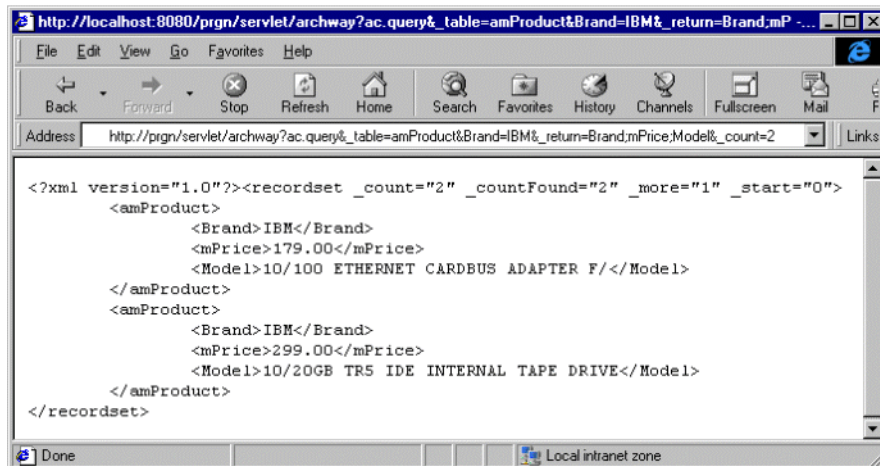
The Document Manager

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 using Get-Answers, you set up users and roles in the system. This chapter describes how to set up Get-Answers so that users can take advantage of its rich feature set.

Topics in this chapter include:

- Users and roles on page 33
- Categories and document ownership teams on page 53
- Managing categories and document ownership teams on page 55
- Configuring Spider (Web crawler) files on page 71
- Integrating Get-Answers with ServiceCenter on page 94
- Using Crystal Reports with Get-Answers on page 113

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 55 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 named System. This Admin user has the rights to configure Get-Answers.

The other is the Administration user named Admin that the Get-Answers adapters require to verify users against the database. This Admin user's database login 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 Admin user interacts with and changes information in the database on behalf of the user.

In the first procedure on , you add a password for the OAA Administration user. In the second procedure beginning on , you add a password for the Administration user that interacts with the database.

Anonymous users

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

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.

Note: This example assumes you are using the default port 80. If you are not
        using the default port, you need to specify the port number,
        `<servername>:8085`, for example.

    ▪   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**.

    A confirmation message appears at the top of the page to confirm that the
    system saved your changes.

Note: Your changes do not take affect until the you click **Reset Peregrine Portal**
        to reset the application server.

6   Click the **Control Panel** link on the left.

7   Click **Reset Peregrine Portal** at the bottom of the page.

    A confirmation message appears at the top of the page.

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 In the Administrator Password field, type the same password you used in step 7.

13 If the Anonymous Login name has the value "admin" or "Admin", then in the Anonymous Password field, type the same password as the one you used in step 7.

14 Scroll to the bottom of the page and click **Save**.

15 Click the **rome** tab.

16 In the Admin Password field, type the same password as the one you used in step 7.

17 If the Anonymous User field has the value "admin" or "Admin", then in the Anonymous Password field, type the same password as the one you used in step 7.

18 Scroll to the bottom of the page and click **Save**.

19 In the Control Panel page that opens, click **Reset Peregrine Portal**.

Note: Your changes do not take affect until you click **Reset Peregrine Portal** to reset the application server.

Important: When 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 for the user named "admin" or "Admin" and the passwords on the rome tab for the user name "admin" or "Admin" 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 group users by capabilities and responsibilities. For example, the Editor role gives anyone assigned that role the permission to read, create, or update documents in a specified document ownership team. Every user in the system is a member of the Default role. In addition, the following roles are included with Get-Answers: Owner, Editor, Reviewer, and Reader.

In general roles are used to:

- Assign duties for the document teams.
- Manage access to document categories.
- Managing document submission to categories.
- Manage access to document fields through document views within roles.

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

See the sections, Document ownership teams on page 53, and Managing categories and document ownership teams on page 55 for more information.

Capability keywords

This section describes how the capability words for menu items are used to control whether or not menu items display. It also provides examples of the role capability keyword strings.

Note: A Get-Answers administrator has the Roles.ga_admin capability word, which is different from the system administrator.

Menu item

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

Menu item	Capability keyword	Role
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, Reviewer, Submitter
Draft Document List	ga.document.new Roles.ga._admin	Owner, Editor, Reviewer, Submitter
Retired Documents	Roles.ga._admin	Admin user (Get-Answers Administrator check box selected on the Security Capabilities page)
Manage Categories	ga.domain.manage	Owner (ga.domain.create to create New Categories; Owner)
Manage Document Ownership Teams	ga.docteam.manage ga.docteam.create	Admin, Owner to create New Teams;
Manage Document Types	ga.manage.doctype	Owner
Shared Content	ga.document.own	Owner, Editor
Import Documents	Roles.ga._admin	Admin user (Get-Answers Administrator check box on the Set Security Capabilities form)
User Settings	ga.document.read	Admin, Owner, Editor, Reviewer, Reader, Submitter, Member
Reconcile Linked Documents	Roles.ga._admin	(Get-Answers Administrator check box selected on the Security Capabilities page)

This screen image shows the menu items managed by the menu item capability keyword for the Get-Answers tab.
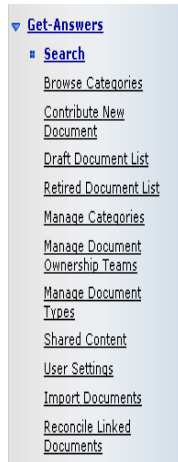
The following code is for the Reports menu items.

Menu item	Capability keyword	Role
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:

Menu item	Capability keyword	Role
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-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;
ga.manage.doctype
```

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;
ga.manage.doctype
```

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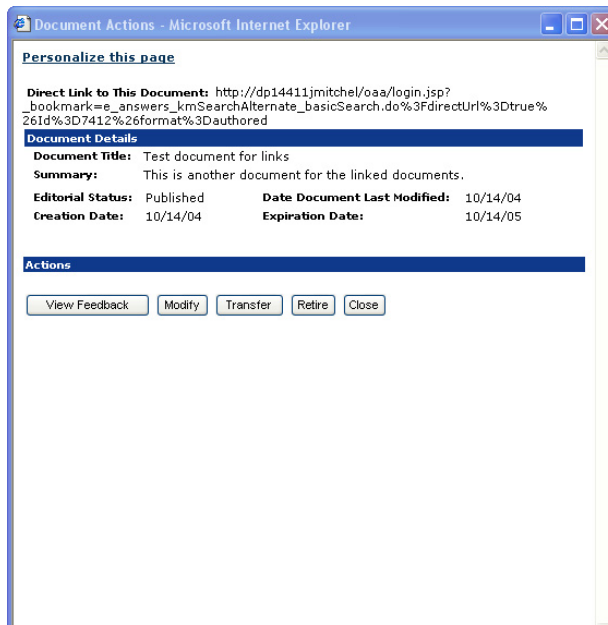
ga.document.own is the necessary permission to view these buttons.

Working with roles

As an administrator, you can create, modify, and delete groups of users by assigning them roles. Although the Functional Roles Details form can be customized to add roles to roles, Get-Answers ignores roles that belong to roles. Use only one level of roles in Get-Answers. The out-of-box roles are Submitter, Member, Owner, Editor, Reviewer, and Reader.

A functional role is a group of people. You could group them according to their job titles or department or the functional tasks that they perform. A person can be associated with any number of roles. In Get-Answers, a document ownership team permission such as Owner, Editor, Reviewer, or Reader is associated with a single person or with a functional role (with a group of people) through the Get-Answers Manage Document Ownership Teams menu item. A category of published documents has Submitters and Member permissions which are associated with a single person or with a functional role through the Get-Answers Manage Categories menu item.

Get-Answers does not use security roles. Security roles are roles that are created with an associated security filter that limits user access to data according to defined business rules within the role entity.

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.

4   Enter a name for the role.

5   Enter a description for the role.

6   Click **Submit** 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. Also, before you can delete a role, you need to ensure that all of the document teams have at least one owner role that is not the role you are deleting.

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.

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.

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

Click Add an item
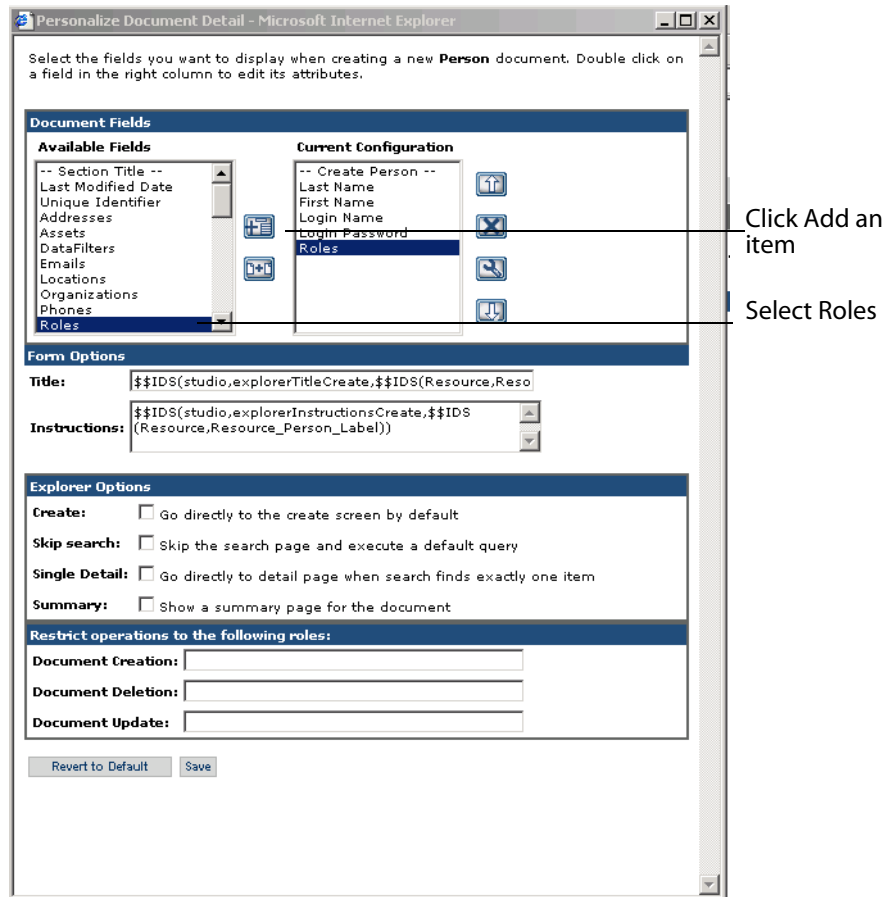
Select Roles

5   Click the **Add an item** icon (plus sign).

    Roles appears in the Current Configuration list.

6   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.

7   Click **Save**.

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.

Note: You must use Personalization to create the Add link on the People Details page before you can assign a role to a user other than the Default role, which is assigned automatically.

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.

3   Type the **Last Name and First Name** for the user.

4   Type the **Login Name**, and **Login Password** for the user.

5   Click the **Account Disabled** check box, if you want to disable access for the new user.

6   Click the **Password Never Expires** check box, if you want to set up this account the Login Password does not expire.

7   Click the **Change Password On Next Login**, if you want the user to select a new password the next time the user logs on.

8   Click **Submit**.

The Person Details page opens.

9   In the Person Details page, you can update any of the current information for this user in the Document Details section or Security section.

10   All users should be assigned at least one role. In the out-of-box version the system assigned the Default role automatically. Click the **Remove** check box to delete this role from the user's profile if you wish.

11   Click the **Add** link in the Roles section to open a search window to search for additional roles defined in the system.

12 Click the search icon.

The Lookup Role window displays a list of roles defined in the system.
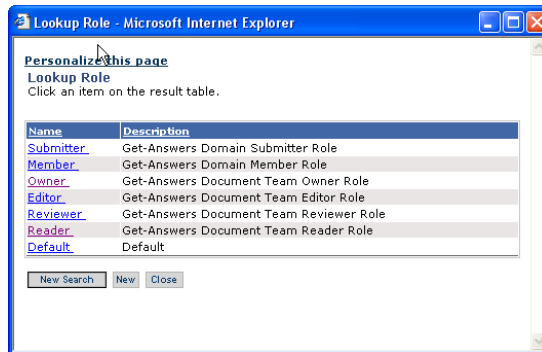
Note: Do not select the Submitter, Member, Owner, Editor, Reader, or Reviewer role on this screen. These Get-Answers roles are assigned using the Manage Categories and Manage Document Ownership functions described in Managing categories and document ownership teams on page 55.

13 Select a role and then click **OK** to close the Lookup Role window.

The Person Details displays the role you selected.

14 You can also click the check box for a role listed in the Roles section to remove it as a role for this user.

15 To add or change the security capabilities assigned to this user, click **Set Security Capabilities** link.

The Set Security Capabilities page appears.

16 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**.

17 Click **Submit Changes** to save the changes you made for this user.

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

The systems returns you to the Person Search Results page where you can click the name of user to verify the changes you made.

Modifying users

Once a user has been added to the system, you can modify the user's profile by changing the information that appears on the Persons Detail page.

To modify a user profile:

1   On the People tab, use the Search function to display the user's profile in the Person Detail.

    The Person Details page opens.

2   Make the desired modifications. See Adding users on page 48 for more details.

3   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:

1   On the People tab, use the Search function to display the user's profile in the Person Detail.

2   In the Person Details page, click **Delete** to remove the user from Get-Answers.

Warning: There may be documents assigned to this user in a workflow. This documents will be orphaned or possibly lost if they are not properly re-assigned to another user.

Categories and document ownership teams

Document ownership teams, which are groups of users 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 team.

When a new document is submitted to a document team, that team owns 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:

Capability	Description
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.

Capability	Description
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:

Role	Role capabilities
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 unpublished documents and create new documents.

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 .

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. Get-Answers comes with the out-of-box category, Get-Answers.

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 team that manages it. A category is owned by one ownership team. Within categories, you can control the document hierarchy by creating categories for your documents.

An unpublished document has no category. A published document is assigned to a category.

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 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.

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

A document ownership must have a specified owner. You create this owner by giving one of the users or some users or a group of users (by assigning users to the role) 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.
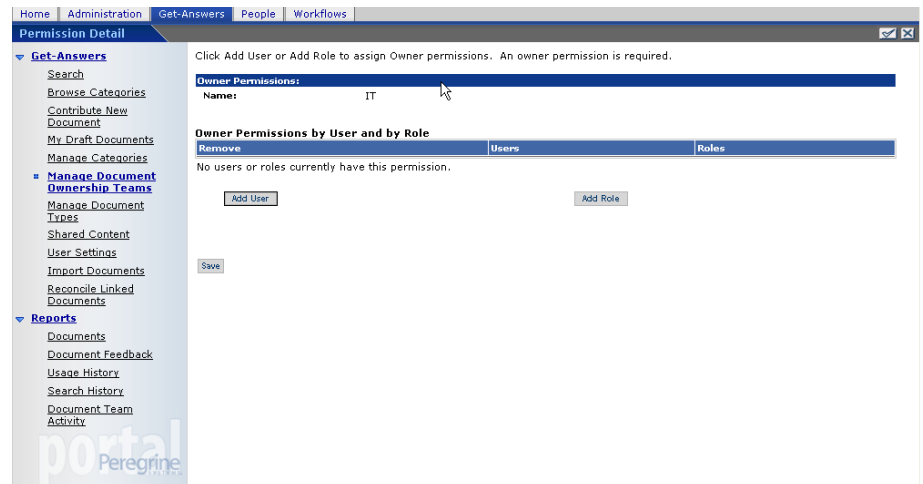
You can document ownership permission for the team by adding roles and users to the team. When you add a role, you are adding all users assigned to that role.

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 to assign.

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. Now you can set Owner, Editor, Review, Reader permissions for the documents owned by this team or you can add these permissions later.

12 Click S**ubmit Changes** to save any changes you make

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:	Technical Publications	

Owned Categories

Name	Description
Technical Articles	

Actions
Set Owner Permissions
Set Editor Permissions
Set Reviewer Permissions
Set Reader Permissions

Submit Changes   Delete

The Permission Detail page opens.

| Home | Administration | Get-Answers | People | Workflows |

Permission Detail

Get-Answers
- Search
- Browse Categories
- Contribute New Document
- My Draft Documents
- Manage Categories
- ■ **Manage Document Ownership Teams**
- Manage Document Types
- Shared Content
- User Settings
- Import Documents
- Reconcile Linked Documents

Reports
- Documents
- Document Feedback
- Usage History
- Search History
- Document Team Activity

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

Owner Permissions:	
Name:	Manufacturing

Owner Permissions by User and by Role

Remove	Users	Roles
Remove	Admin, System	
Remove	user, super	

Add User   Add Role

Save

2   To add a role to the team, 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 name link in the list.

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

5   To add users to the team, click **Add User**.

The Search for Users page opens.

6   Click **Search** or type the name of the user.

The List of Users page opens.

7   Click the user name link in the list.

8   The Permission Detail page opens with the user you selected listed in the Owner Permissions by User and by Role section.

9   Click **Save** after you have added all of the users and roles for the team.

The Document Team Detail page opens.

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

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

and repeat steps 2 to 9 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.

11 Click **Submit Changes**.

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 **Submit Changes**.

Note: For details on document team options, see Adding document ownership teams on page 56.

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   Click the name of the document team in the list you want to delete.

The Document Team Detail page for the team opens.

4   Click the **Delete** button.

The Delete Document Team page opens.

5   Click **Delete Document Team** to remove the document team.

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

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.

2   Click **New**.

The Category Detail page opens.

3   Enter a **Name** for the category.

4   Enter a description of the category in the **Description** field.

5   From the drop-down list, select the managing document team for the category.

6   Click **Save**.

The Category Detail page opens. The Name, Description, and Document Team fields are filled in. You can modify this information or add additional category details.

7   In the Category Hierarchy section, type a **New Subcategory**. Remember to select the appropriate category or subcategory for the category or subcategory you are creating.

8   Click **Insert** to add the category or subcategory.

You can create multiple subcategories for a category, depending upon the complexity of the category and how you want to organize the documents in the category.

9   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.

10 Click Submit Changes to save your new category or go to Actions section to update the submitter and member permissions.

Adding submitter permissions to 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 submit 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.

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

1   Click the **Set Submitter Permissions** link.

The Permission Detail page opens.

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   In the list of roles returned by the search, click the role are adding, 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 a user to submitter permission for the category.

6   In the Search for Users page, enter the name of the user you want to add and click **Search**.

7   In list of users returned, click the user name.

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

8   Click **Save**.

     You are returned to the Category Detail page.

9   Click **Submit Changes** to save the category details.

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**.

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 **Submit Changes**.

Note: For details on the category options, see Adding, changing, or deleting categories on page 62.

Deleting categories

You can only delete a category or a subcategory that has not published documents in it or subcategories in it.

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 62 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 New Subcategory text box, select the parent category or subcategory and then click **Insert**.

- To delete a subcategory, click the subcategory in the list on the right and click **Delete**.

- To change the name of a subcategory:, select the subcategory, click **Update**, type the new name in the text box provided, and click **Submit Changes**.

Note: You cannot rename a category.

6   Click **Submit Changes**.

The message "Changes successfully saved" appears at the top of the page.

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.

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, **Get-Answers Search Engine Internet Spider Utilities**.

    d   In the order listed on the menu, start the O2 server (2), then the URL server (3).

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 displays the URLs being crawled. Then the search engine indexes 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, **Get-Answers 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 **1**s.

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.

   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   Select option 14, **Get-Answers Search Engine Internet Spider Utilities**.

   d   Select option 2, **Start O2 server**.

   e   **Exit** from **System Utilities** by entering a series of **1**s.

Spider configuration files

A Spider library has several configuration files.

File	Description
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
afm_libpath	Specifies the path to the AFM library files being used by Spider. The default is SPIDERHOME/bin.
afm_loglevel	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).
afm_lst	Specifies the path to the afm.lst file being used by Spider. The default is SPIDERHOME/spider-lib/config/afm.lst.
afm_rul	Specifies the path to the afm.rul file being used by Spider. The default is SPIDERHOME/afm.rul.
conn_timeout	Specifies the number of idle seconds before Spider disconnects the socket connection to the HTTP/FTP server. The default is 20 seconds.
follow_redirect	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.
index_waiting_time	When the storage_path parameter is not specified, this parameter determines how long tproc 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, tproc will wait for the number of seconds calculated by the following formula (where doc_length is in KB): index_waiting_time*floor(doc_length (KB)/256) For example, if the index_waiting_time is 2 and the size of the document is 2 MB, then the waiting time is 2 * floor (2*1024/256) = 16 seconds. The default is 2.
local_cookies	Specifies how to manage cookies: 1=manage cookies locally (per module basis); 0=use cookies passed in as parameters. The default is 0.
min_cache	Specifies the minimum database cache size in megabytes. The default is 64.
nfile_hashdbm	Specifies the number of underlying database files for the VISDIS filter database. The default is 5.

Parameter	Description
nsync_read_initurls	Spider parses this number of starting URLs in the main thread and then starts the tfetcher (starts crawling). Spider then launches the thread to parse the rest of the URLS in the initial URL file. This thread will sleep for waittime_nonsync_read seconds after it's done processing every nsync_read_initurls URLS. The default is 100.
process_ftp_dirlist	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.
rware_name_server	Specifies the host name and port number of a remote RetrievalWare (search engine) name server for Spider to connect to. (Example: rware_name_server: rwhost:6000)
use_host_distance	Enables or disables the host distance filter (host_distance). Use 1 or on, 0 for off. The default is 1.
use_url_distance	Enables or disables the distance filter (url_distance). Use 1 or on, 0 for off. The default is 1.
verbose	Specifies a level for the types of messages that appear in the log files for tagent and tproc. 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.
waittime_nonsync_read	See nsync_read_initurls 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.1st` 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.1st` 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 intersection (M(strong_allow) union (M(allow) minus M(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 links(u) is all the URLs referenced by u, then all URLs in A(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 93 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**
change_revisit	1	URLs that were new or had changed on the last visit.
access_denied_revisit	5	URLs that were denied due to invalid or no user ID or password.
extinct_revisit	30	URLs that were marked bad by HTTP return code (404, for example) on the last visit.
moved_revisit	0	URLs that were marked moved by HTTP return code (301, 302) on the last visit.
timed_out_revisit	5	URLs that timed-out during the last transfer.
transfer_error_revisit	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
retrieve_once	none	Retrieve the URLs that match the regular expression only once during the lifetime of the Spider database.
retrieve_always	none	Retrieve and re-index URLs that match the regular expression on every crawl.
retrieve_frequency: #:	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, retrieve_frequency: 5.0: http://www\.example\.com/ means retrieve the "example site every 5 days.
retrieve_normal	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, todays_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/todays_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.1st` 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.1st` 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.1st`, 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
^	Regular expression must match from the beginning of the string.	`^http` : matches all strings beginning with `http` :
$	Regular expression must match at the end of the string.	`html$` matches all strings ending in html
\	Negates all special meaning for the following character.	`\$` matches the `$`character
.	Matches any 1 character	`welcome.` matches welcome1, welcomeb, welcome? and any other string with welcome followed by any 1 character
*	Matches 0 or more of the preceding characters.	`welcome*` matches welcom, welcome, welcomee, welcomeee, etc.
+	Matches 1 or more of the preceding characters.	`welcome+` does not match welcom, but does match welcome, welcomee, welcomeee, etc.
?	Matches 0 or 1 of the preceding characters.	`html?` matches only htm and html.
[]	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
csh or tcsh       > setenv SOCKS_SERVER 123.45.67.8
ksh or bash       > export SOCKS_SERVER=123.45.67.8
```

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 -dbclear.`

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 ServiceCenter

This section outlines the procedures for integrating Get-Answers with ServiceCenter 6.0.x.

Note: If you are not using Get-Answers as a knowledge base for ServiceCenter, you can skip this section.

Configuring your Get-Answers and SeviceCenter integration

Follow these steps if you are configuring your Get-Answers and ServiceCenter integration

ServiceCenter integration changes

1   You need to remove the original Display Options setting for Get-Answers.
    The original Display Options for Get-Answers are the Display Options
    provided with the out-of-box ServiceCenter.

    a   In ServiceCenter, select **Utilities** > **Tools** > **DisplayOptions**

    b   In Default Label type with "Get-Answers."

    c   Click **Search**.

    d   Click **Mass Delete**.

2   Load the file sc60ga.unl.

    a   Navigate to T**oolkit** > **Database Manager**.

    b   Use the menu drop-down to select **Import/Load**.
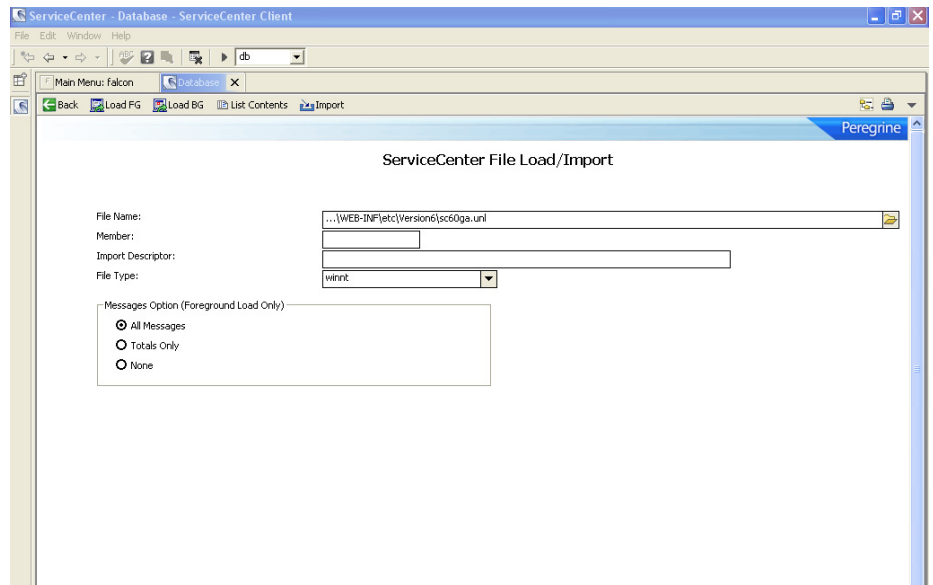
    c   Browse to location of file unload, sc60ga.unl
        (<deploy_root>/WEB-INF/etc/version6/).

    d   Click **Load FG**.

    e   A verification message appears.

    \...\WEB-INF\etc\Version6\sc60ga.unl file loaded.

3   Configure the System wide company record.

    a   Navigate to **Utilities** > **Administration** > **System Wide Company Record**.

    b   Click the Active Integration tab.

    c   Click the **Get-Answers** check box.

    d   Type in the Base URL text box the base URL for your Get-Answers application. If the Base URL text box contains a default value, replace it with the correct URL.

    e   Example: *http://<get-answers server>:<port>/<get-answers virtual dir>/*

Note: The <port> is required only when the default port number is not being used.

    f   Click **Save**.

4   To utilize the Audit Trail feature, you must remove delays when assigning ID numbers for Incident Management (IM).

   a   Navigate to **Toolkit** > **Database Manager**.

   b   Search for environment.

   c   Open record, environment.pm.

   d   Uncheck **Delay Assigning Incident Number**.

   e   Click Save.

5   Log off from ServiceCenter and then log on for the changes to take effect.

You can repeat this procedure for the for environment.sm if this has been changed from the out-of-box ServiceCenter installation.

Adding custom retrieval solutions

To create or customize a Retrieve Solution mapping for the Get-Answers integration with ServiceCenter:

1   Fill in or modify the field in Retrieval tab of the Get-Answers Configuration Record.

2 This is done to an existing mapping or new mapping record depending on your implementation requirements.

The following is a screen capture of the Retrieval tab of the Get-Answers Configuration Records screen.
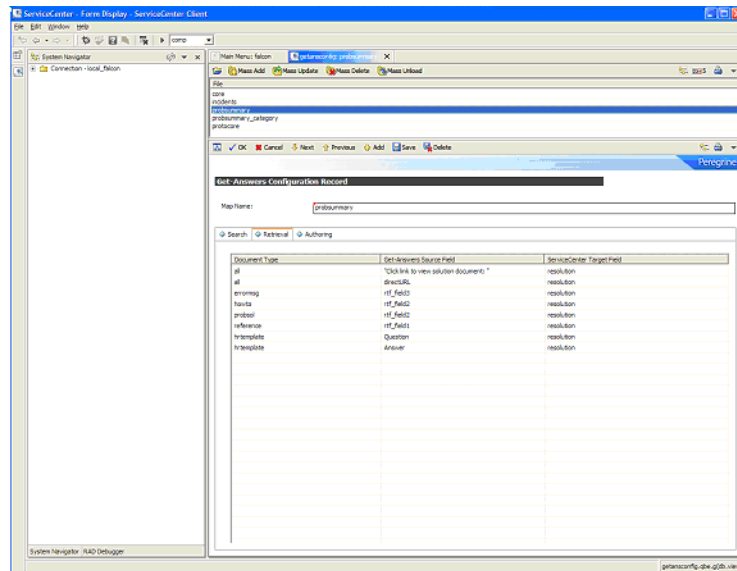
3 Make the following updates as required.

- The **Map Name** field is the name of the mapping. By default the out-of-box mappings are named according to the ServiceCenter file name they provide a mapping for. If a Map Name other than the ServiceCenter file name is used, the thread variable $gamapname must be set to the value of the **Map Name** from the Display Option used to call the mapping. (see Creating custom search mappings on page 106)

- The **Document Type** column specifies the Get-Answers document type that is the source of the Retrieve Solution request. The value specified in this column MUST match the Storage Value field of the Get-Answers Document Type from which you wish to retrieve. A value of all can be specified to indicate that the field mapping will be used for all document types.

- The **Get-Answers Source Field** column specified the field (as defined in the rKmDocument schema in Get-Answers) used to retrieve data from for the Document Type listed in the corresponding row. A literal string

value can be specified in quotation marks. Any string of characters specified within quotation marks are copied literally (without the quotations) into the ServiceCenter Target Field.

▪ The **ServiceCenter Target Field** column specifies the field in ServiceCenter that receives the data retrieved from the Get-Answers Source Field. If a ServiceCenter field is the target for more than one Get-Answers field, the data is appended (in the order specified in the mapping) into the ServiceCenter Target Field.

Adding custom authoring

To create or customize an Author Solution mapping:

1 Complete or modify the field in Authoring tab of the Get-Answers Configuration Record.

2   This is done to an existing mapping or new mapping record depending on your implementation requirements.

The following is a screen capture of the Authoring tab of the Get-Answers Configuration Records screen.
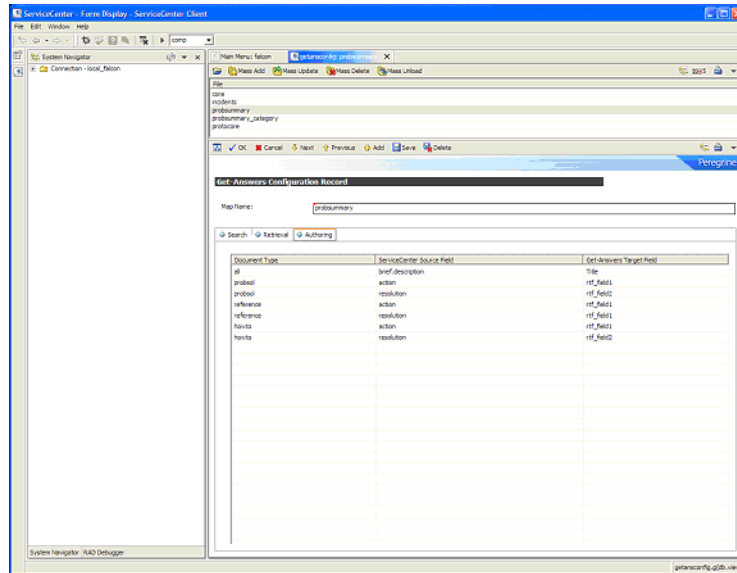
3   Make the following updates as required.

- The **Map Name** field is the name of the mapping. By default the out-of-box mappings are named according to the ServiceCenter file name they provide a mapping for. If a Map Name other that the ServiceCenter file name is used, the thread variable $gamapname must be set to the value of the Map Name from the Display Option used to call the mapping. (see Creating custom search mappings on page 106)

- The **Document Type** column specifies the Get-Answers document type that is the target of the Author Solution request. The value specified in this column MUST match the Storage Value field of the Get-Answers Document Type for which you wish to Author. A value of **all** can be specified to indicate that the field mapping will be used for all document types.

- The **ServiceCenter Source Field** column specifies the field in ServiceCenter that provides the source data sent to the Get-Answers Target Field. A literal string value can be specified in quotation marks.

Any string of characters specified within quotation marks is copied literally (without the quotations) into the Get-Answers Target Field.

- The **Get-Answers Target Field** column specifies the field in Get-Answers (as defined in the rKmDocument schema in Get-Answers) that receives the data sent from the ServiceCenter Source Field. If a Get-Answers field is the target for more than one ServiceCenter Source field, the data is appended (in the order specified in the mapping) into the Get-Answers Target Field.

Adding custom document types for authoring

To add custom document types for authoring:

1   In the Database Manager, search for **getansdoctype**.

2   Open the form **getansdoctype** with a single text field on it.

3   Click the **Search** button to display a list of currently supported document types for authoring.

4   Open by double-clicking a document type to display form called getansdoctype with a single text field on it that is filled in with the type you selected.

5   Change the document type name.

6   Click the **Add** button. Save replaces and Add creates a new document type in the list.

    A confirmation messages appears stating that a record was added.

7   Click **OK**.

    This re-displays the list (the new document type does not appear in the list).

8   Click **Refresh**.

    The list appears with the record you added.

Adding custom search configurations

To create or customize a search mapping:

1 Complete or modify the field in the Search tab of the Get-Answers Configuration Record.

2 This is done to an existing mapping or new mapping record depending on your implementation requirements.

The following is a screen capture of the Search tab of the Get-Answers Configuration Records screen.
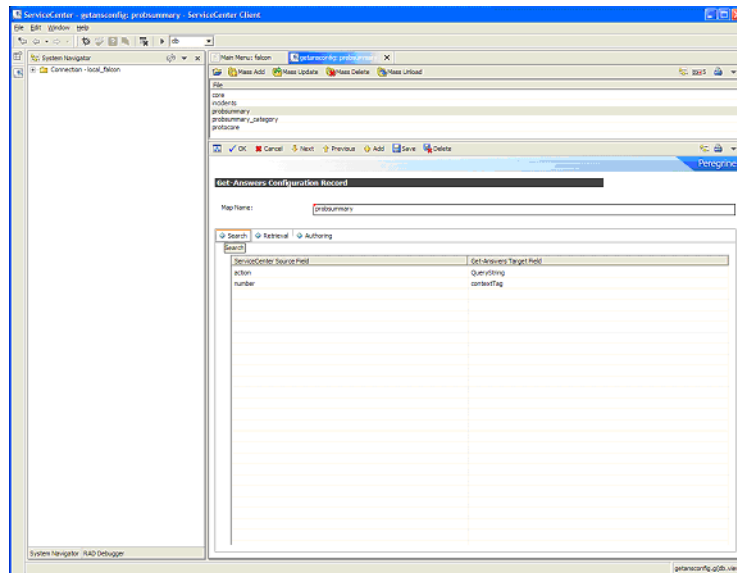
3 Make the following updates as required.

- The **Map Name** field is the name of the mapping. By default the out-of-box mappings are named according to the ServiceCenter file name they provide a mapping for. If a Map Name other that the ServiceCenter file name is used, the thread variable $gamapname must be set to the value of the Map Name from the Display Option that is used to call the mapping. (see)

- The **ServiceCenter Source Field** column specifies the field in ServiceCenter that is sent to the Get-Answers Target Field. A literal string value can be specified in quotation marks. Any string of characters

specified within quotation marks is copied literally (without the quotations) into the Get-Answers Target Field.

- The **Get-Answers Target Field** column specifies the field in Get-Answers (as specified in the kmSearchFields schema) that receives the data sent from the ServiceCenter Source Field. If a field is specified as a target for more than one ServiceCenter Source Field, the data from the source field is appended (in the order specified in the mapping) into the target field. A value of "QueryString" specified in this column indicates that the data from the source field is sent as part of the non-fielded search string (such as if a user typed into the "Enter your question" box in the Get-Answers search interface). A value of "contextTag" is used to indicate that the source field value will be used to track all search activity for later viewing in the Audit Trail feature. This is the ticket number for Calls and Incidents.

Get-Answers integration changes

To configure Get-Answers for integration with ServiceCenter the users in ServiceCenter that are going to need access to Get-Answers need to exist in both systems with the same logons.

Note: There is a Connect-It scenario that you can use to synchronize the users in Get-Answers and ServiceCenter. The Connect-It scenario is in the `SupportFiles/DatabaseFiles` folder on the CD.

To configure Get-Answers for integration with ServiceCenter:

1   Log on the Get-Answers as an administrator.

2   On the Administration tab, click the **Settings** link in the Control Panel menu.

3   Select the Get-Answers Portal tab.

4   In the List of target aliases text box, add **sc** to the list of aliases.

5   Click **Save**.

A confirmation massages confirms that your setting has been changed. You now need to reset the server for the change to take effect.

6   Click the **Control Panel** link in the Admin Settings menu.

7   Click the **Reset Peregrine Portal** button on the Control Panel page.

A confirmation message appears when the server reset completes.

You can now verify that a ServiceCenter user can search the Get-Answers knowledge base for a solution as part of processing an incident.

Note: You need to setup the ServiceCenter tab (Get-Answers, Admin Settings page) if you have not already configured it.

To setup the ServiceCenter tab:

1   From the Peregrine Portal Admin module, click Settings.

2   At the top of the Settings page, click the ServiceCenter tab to open the ServiceCenter settings page.

3   Update the following fields.

Field Name	Value Description	Default Value
Host	Host name of the ServiceCenter server.	localhost
Port	Port number of the ServiceCenter server.	12670
Log	The path to SC logging that the ServiceCenter client connection uses	(none)
Admin user	Administration login name that the Peregrine Portal uses when performing tasks such as user authentication and registration	falcon
Admin password	Administrator password	(none)
Anonymous user	Name to use when unknown user attempts to connect with ServiceCenter	falcon
Anonymous password	Anonymous user password for ServiceCenter	(none)
Default capabilities	Access rights for all users.	(none)
Adapter	Full class path for adapter associated with this target	`com.peregrine.oaa.` `adapter.sc.SCAdapter`
`WEB-INF/bizdoc/Enum` `/SysEnums.xml`	The xml file that provides the values for enumeration data types	(none)

4   When finished, click Save.

5   Click **Control Panel** > **Reset Peregrine Portal** to apply your changes to the system.

Verifying ServiceCenter integration with Get-Answers

To verify that this integration is working properly, create at least one document in Get-Answers that suggests a solution to a problem. For a detailed explanation of using Get-Answers as a knowledge base for ServiceCenter, see Chapter 4, Using Get-Answers with ServiceCenter integration in the *Get-Answers User's Guide.*

Creating custom search mappings

You can create additional mappings between Get-Answers and ServiceCenter of the ServiceCenter categories to the Get-Answers categories. This allows users to do document searches in Get-Answers that include filters based on the categories defined in ServiceCenter. In order to do this, the category names must match between Get-Answers and ServiceCenter.

To create custom mappings:

Note: This example illustrates how to create a new mapping for a probsummary_category.

1   In ServiceCenter, navigate to the System Information Definition form for the System Wide Company Record.

2   In the drop-down menu, select **Get-Answers Configuration Records**.

The Get-Answers Configuration Record form opens.

3   In the list of files, select the probsummary file.

4   In the Map Name field, type **probsummary_category**.

5   In the ServiceCenter Source Field type **category**.

6   In the Get-Answers Target field type **CategoryName**.

7   Click **Add** to create the new record.

Next you need to create a new display option to call this mapping. You must set the $gamapname thread variable to the name of the mapping you just created.

To create a new display option:

1   In ServiceCenter, navigate to Display Options: select **Utilities** > **Tools** > **DisplayOptions.**

2   Create a new display option for the form you customize with the search.

3   In the Default Label text field, type **Get-Answers>Search Solution by Category**.

4   In Expressions are evaluated after option is selected, but before RAD call, type the $gamapname thread variable, **$gamapname="probsummary_category"**.

5   Update the other fields as required.

6   Click **Add**.

7   Verify that the Get-Answers sub-menu on the ServiceCenter drop-down menu displays Search Solution by Category.

Limiting viewing of the Audit Trail menu item

This section explains how to limit users from viewing the Audit Trail menu item in ServiceCenter when using Get-Answers with ServiceCenter.

To limit users from viewing the Audit Trail menu item:

1   In ServiceCenter, add a new capability word (ex: getanswers.audittrail).

2   Assign the new capability word to the users or roles you want to access the Audit Trail.

3   Edit the Display Option for **Get-Answers** > **Audit Trail**.

   ▪ Go to Display Options search screen and enter **Get-Answers**>**Audit Trail** in the Default Label field.
   ▪ Search

4   Specify the condition as `gui() and nullsub(GetAnswers in $G.system.info, "false") and index("getanswers.audittrail", $lo.ucapex) > 0.`

Importing users from ServiceCenter to Get-Answers

Get-Answers 4.2 contains two Connect-It scenarios that allow administrators to import Contacts from ServiceCenter into the Get-Answers *rPerson* table. These scenarios serve as working templates for importing users from ServiceCenter to Get-Answers. Get-Answers administrators can modify these templates to fit the needs of their implementation. If your implementation requires importing Operators instead of Contacts, you can modify these scenarios accordingly. These scenarios are available on the Get-Answers 4.2 product CD in the Support Files folder and require Connect-It version 3.3.2 or later.

The first scenario is the `sc2oaa_insert.scn` file. This scenario inserts Contacts that do not already exist in the *rPerson* table. All Contacts added to the *rPerson* table are assigned to the Default Role. The second scenario is the `sc2oaa_update.scn` file. This scenario updates Contact information for Contacts that already exist in the *rPerson* table.

Configuring the sc2oaa_insert scenario

To configure the sc2oaa_insert scenario:

1   Copy the `sc2oaa_insert.scn` file to a location accessible by Connect-It.

2   Launch Connect-It version 3.3.2 or later.

3   From the File menu, select Open and the choose `sc2oaa_insert.scn` from the location in step 1.

4   Right-click the Bizdoc-Archway box in the Scenario diagram window and
     then select Configure connector from the popup menu.
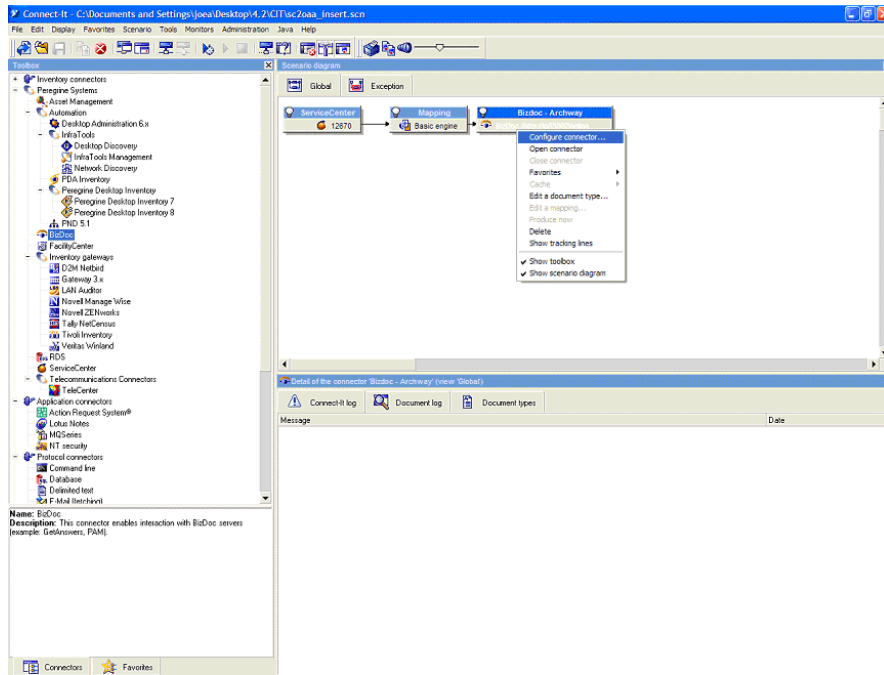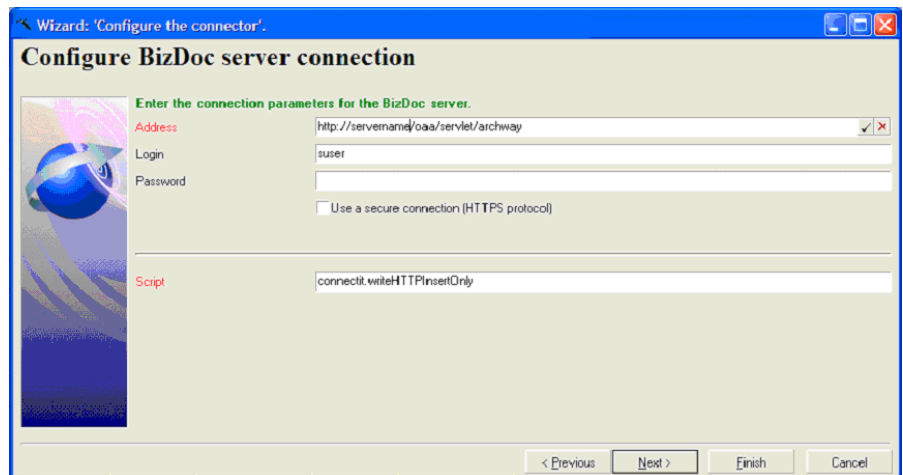
5   On page 2 of the wizard, select the **Write** radio button.
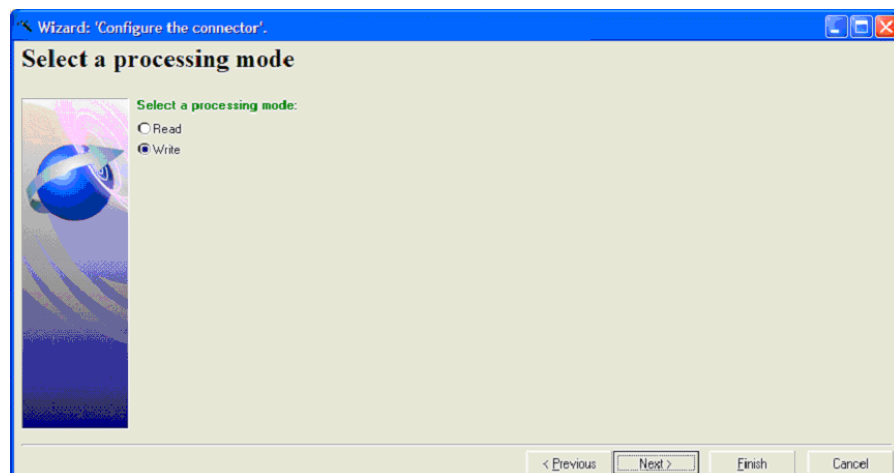
6   Go to page 3 of the wizard and complete the Address field with the base URL to the Get-Answers server followed by "/servlet/archway."

Example: `http://servername/oaa/servlet/archway`.

7   Complete the Login and password fields with the login and password for an account on the Get-Answer server that has the capability to insert and update People and Roles. The scenario is preconfigured to use the suser account but the password must be provided.

8   Go to the fourth page of the wizard (setting DSD folder) and complete the DSD field.
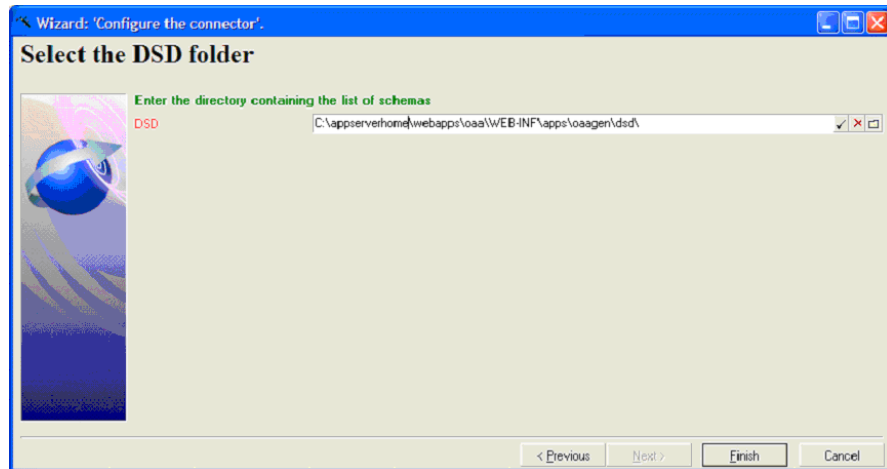
9   Click **Finish** and save the scenario.

Configuring the sc2oaa_update scenario

To configure the sc2oaa_update scenario:

1   Copy the `sc2oaa_update.scn` file to a location accessible by Connect-It.

2   Launch Connect-It version 3.3.2 or later.

3   From the File menu, select Open and choose `sc2oaa_update.scn` from the location in step 1.

4   Follow the steps 4 through 9 in .

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, `jcinst.exe`.

3   Start your Web browser with the following address:

    *http://<Get-Answers server>/oaa/login.jsp?_bookmark=
    e_answers_kmSearchAlternate_basicSearch.jsp?DDEType=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 matrix 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:

Report	Description
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.

Report	Description
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 report 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 standardize 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

CHAPTER

Using the Peregrine Portal

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.

Topics in this chapter include:

- Logging in to the Peregrine Portal on page 115
- Using the Activity menu on page 117
- Personalizing the Peregrine Portal on page 118

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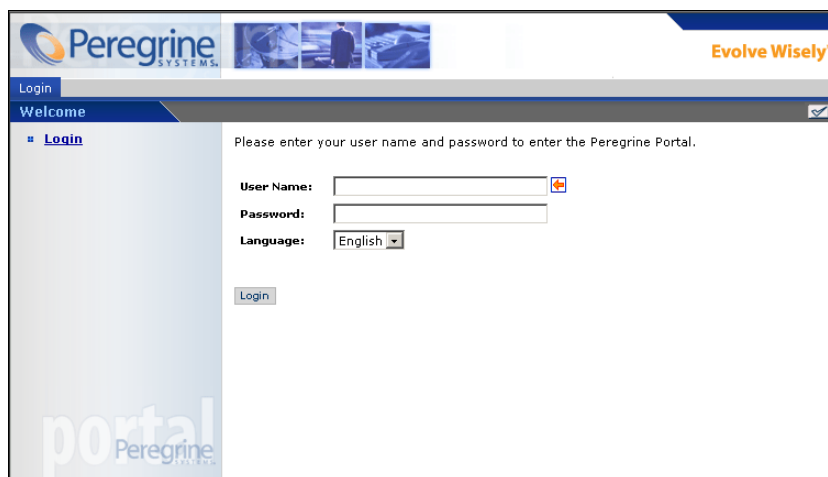
There are two login screens that provide access to the Peregrine Portal:

Login screen	URL
User login	*http://<server>/oaa/login.jsp*
Administrator login	*http://<server>/oaa/admin.jsp*

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

Note: 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. Enter your user name
and password. In the Language pull-down list select the language that you want
the Peregrine Portal to display. English is the default login language, but you can
enable other languages in the Settings page of the Administration Control
Panel. For more information about enabling login languages, see the section
Choosing a Login Language.

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.

Activity menu   Navigation menu   Personalize your   End your
                                                    Home page   session
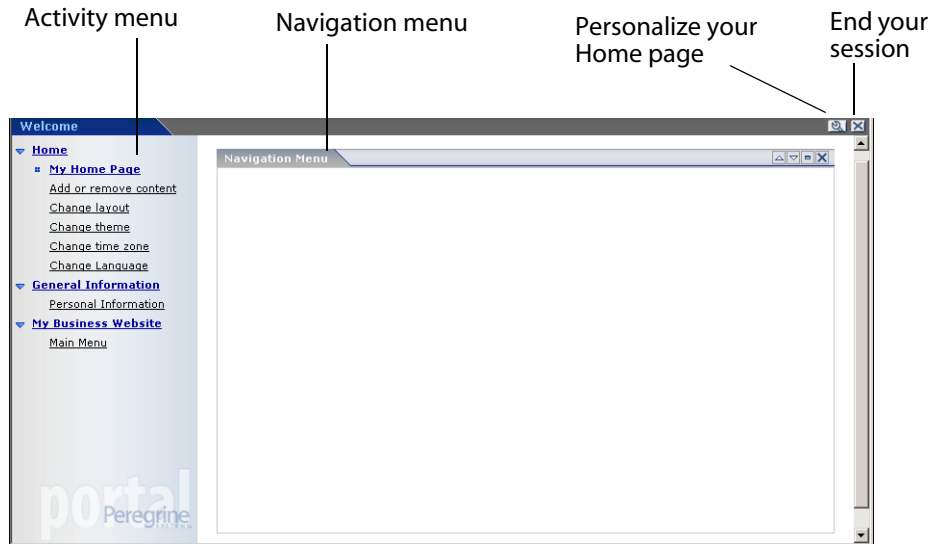
Using the Activity menu

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.
Get-Answers Search Portal	Displays a search window for Get-Answers.

Note: The Calendar and Calculator require Microsoft Internet Explorer 6.0+ 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 with a list of the components available for customizing.
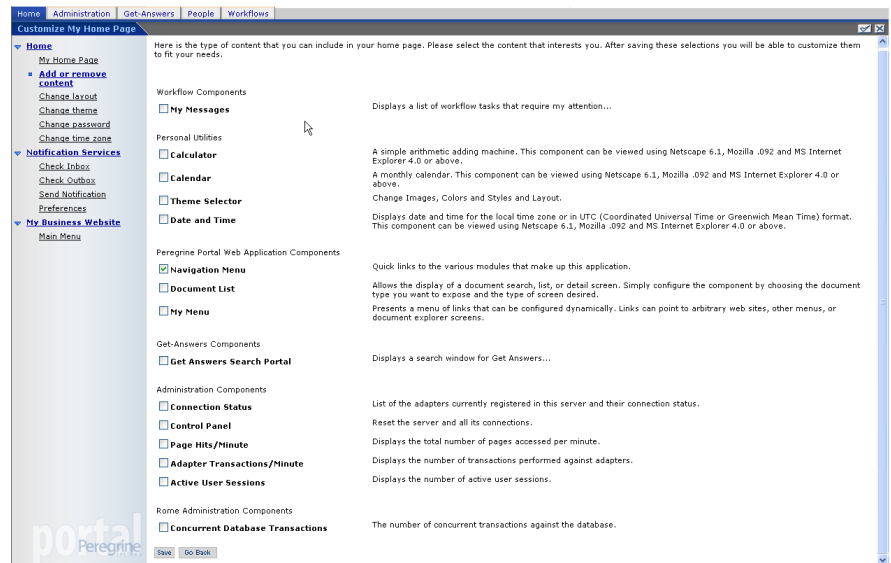
2   Select the components you want to either add or remove from your
    Peregrine Portal.

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 appear in the
    Peregrine Portal. The following example shows the Calendar and Calculator
    added to the Portal.
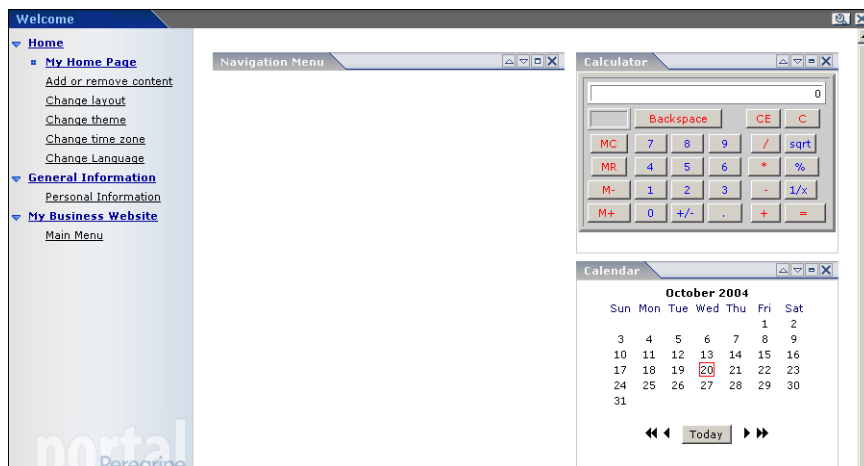
Changing the layout

The following sections contain procedures for changing the location of the components or removing them from the Peregrine Portal. Your Web browser determines the procedure you use.

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.

Move
component up

Hide/Show component
detail

Remove
component

Move component down
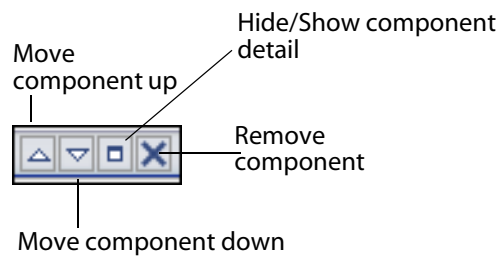
The following screen shows the Calculator hidden or minimized.
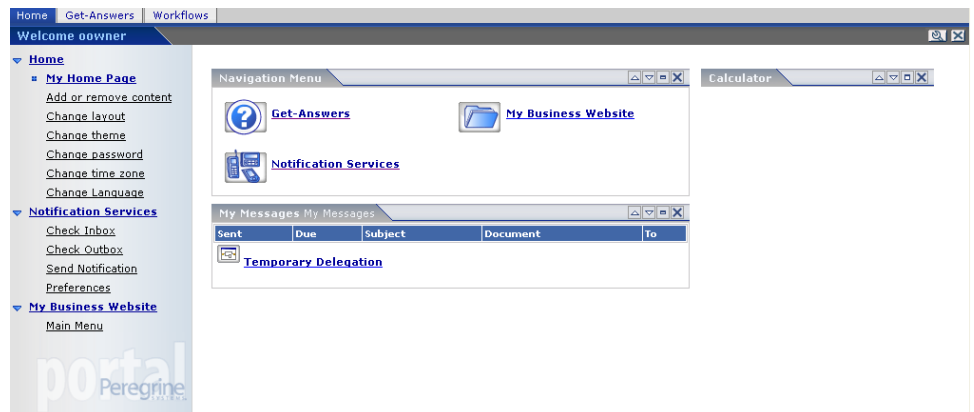
Netscape Navigator

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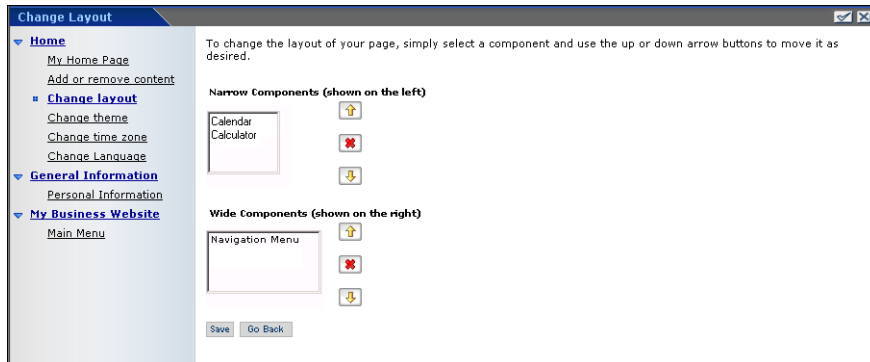
Components can be Narrow (for example, Calendar or Calculator) and are on the left side of the Peregrine Portal. Other components (for example, Navigation Menu) are Wide and are on the right side of the Peregrine Portal.

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. The of-the-box installation provides several themes from which you can choose. 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**.
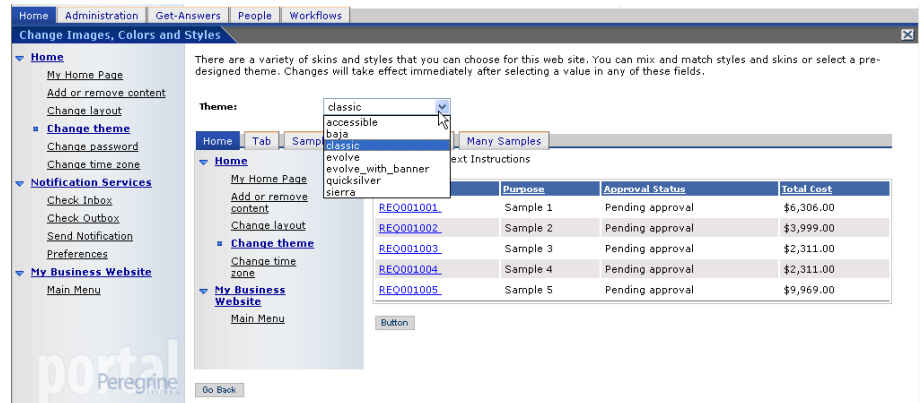
2 Choose a theme from the drop-down list.

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 for the user until changed by the user.

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.
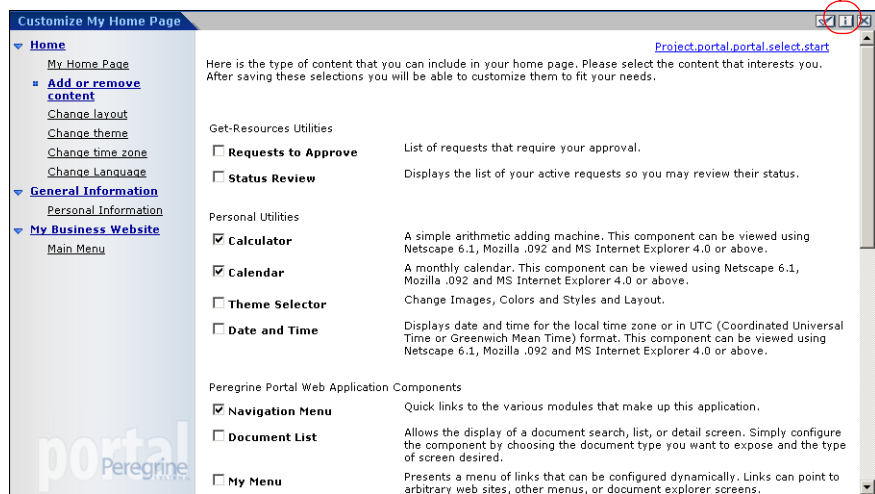
4 CHAPTER

Customizing the Peregrine Portal

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 Get-Answers 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
- Changing the default theme
- Changing the header graphic for all themes
- Creating a custom theme
- Layers properties
- Changing framesets
- Creating script extensions
- Translating Get-Answers

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 screen shots 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:

Theme	Description
Accessible	Makes the screen available to users who need high contrast colors or better accessibility support. It provides 508 compliance.
Baja	Adds southwestern green and beige hues to the Classic design.
Quicksilver	Adds silver and blue hues to the Classic design.
Sierra	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-box the default theme is classic.

To change the default theme:

1   Open your Web browser and log in to the Admin module (`localhost/oaa/admin.jsp`) as the system administrator.

2   Click **Settings** > **Themes.** Change the following parameters:

■   In the **Default skin/Theme** field, change the parameter to the name of the theme you want to use (for example, *Baja*).

■   In the **Default style sheet** field, change the parameter to the appropriate name for the CSS file (for example, `baja.css`).

■   In the **Default XSL templates** 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   Click the **Control Panel** link on the Admin Settings menu.

5   When the Control Panel opens, click **Reset Peregrine Portal**.

6   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 Get-Answers 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 132.

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 138.
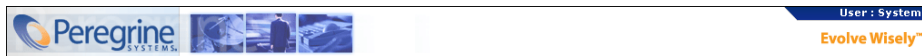
2   Save your custom header graphic to the following location:

    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, type the name of your custom header logo.

Type your new image name.

6   Scroll to the bottom of the page, and then click **Save**.

7   Click the **Control Panel** link on the Admin Settings menu.

8   When the Control Panel opens, click **Reset Peregrine Portal**.

9   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, style sheets, and XSL templates. These files are located at:

File type	Location
Images	`<application server>\oaa\images\skins\classic`
Style sheets	`<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`
Style sheets	`<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.
.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 style sheet colors match your image colors.

Note: You can see a detailed style sheet key in the themes Administration section of the Portal. To access the style sheet key, locate the Default style

sheet field on the Themes tab of the Admin Settings page and click the
Peregrine Portal Stylesheet Key link.

5 Save your theme style sheet 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, see Layers properties on page 136.

7 Open and edit any XSL style sheets you want to change.

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

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

The following table lists the XSL style sheets you can change.

To change	edit this XSL stylesheet
Attachment picker	attachments.xsl
HTML form generation	basic-form.xsl
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.
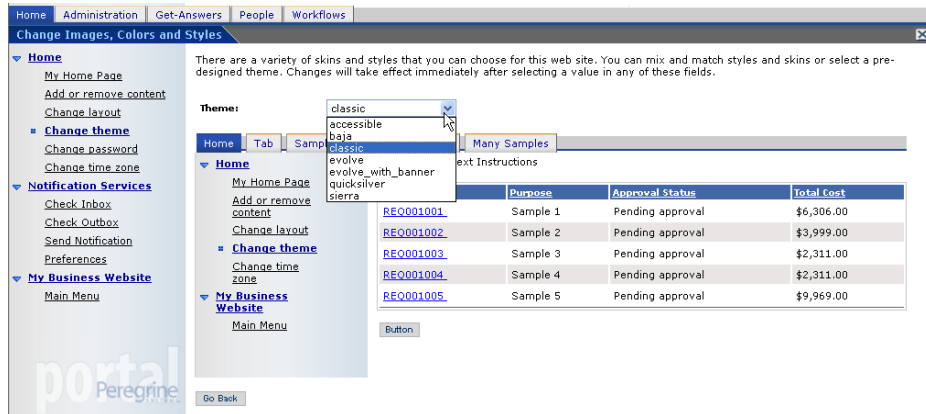
Layers properties

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;">
<img name="logo" border="0" src="<%= logo %>" alt="logo"></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%"> </td>
<td nowrap width="3" align="right" valign="top">
<img src="<%= Archway.getSkinImagePath("backgrounds/rt_l.gif",
user ) %>">
</td>
<td nowrap align="right" valign="top" width="100%"
background="<%=
Archway.getSkinImagePath("backgrounds/rt_tile.gif", user ) %>">
<img src="<%= Archway.getSkinImagePath("backgrounds/rt_tile.gif",
user ) %>">
</td>
<td nowrap><font class="userBarText" size="1" face="Arial,
Helvetica, sans-serif"><%=userTitle%></font>  </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;"> 
</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>
```

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="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_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>
```

Creating script extensions

By creating ECMA script extensions, you can modify the actions of the out-of-box script without changing the original script. Extension scripts are added to the `jscriptextensions` directory under `WEB-INF/apps/<component>`, where `<component>` is the name of an application module (for example, `common`, `portal`, and so on).

When adding extension scripts, you must:

- Preserve the hierarchy (path) of the out-of-box script under the `jscriptextensions` directory.
- Use only one extension per OAA `.js` file.

The extension file can declare new functions as well as functions that override functions of the same name in the out-of-box file. The object created to represent the out-of-box file is configured as the *prototype* object of the extension object.

You can call original function implementations from a function that overrides the original by appending `proto` to the function reference. For example, to call the out-of-box implementation of `login.login()`, use `proto.login.login(msg);` from the `login()` method declared in the extension file.

The following example writes a message to the archway log when the user logs in.

```
function login( msg )
{
   env.log("*** YOUR MESSAGE GOES HERE*** ");
   return proto.login.login(msg);
}
```

Note: The relative path of the example extension file is
       `..\WEB-INF\apps\common\jscriptextensions\login.js`.

If the out-of-box method calls other functions that are also overridden in the extension file, use the following technique to ensure that the new implementations of the secondary functions are called:

```
proto.login.login.apply(this, arguments);
```

where `arguments` is an implicit variable that exists in the context of an ECMA Script function.

```
function login( msg )
{
   env.log("*** YOUR MESSAGE GOES HERE*** ");
   return proto.login.login.apply(this, arguments);
}
```

Translating Get-Answers

Out-of-box, all Peregrine OAA web applications are provided in English. You can download the Get-Answers language pack from the Peregrine Customer Support Web site 90 days after the English release. For Get-Answers language packs are free. Language packs are available for the following languages:

- French
- Italian
- German

Note: Not all Peregrine OAA web applications 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 Get-Answers, you need to add the Locale field to four of the sample document creation screens.

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 143.

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 string files on page 144.

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 145.

Adding the Locale field to document creation screens

If you are deploying the FIG (Internationalization) release, add the Locale field to every Document creation screen except for External Document Type creation screens. This Locale field is necessary to expand search terms in the correct language.

For each of the Document Types (except External), complete the following steps:

1   One by one, open each Document creation screen for that Document Type. Find these by selecting **Contribute New Document** and then selecting the document type.

2   Click the **Personalization** wrench icon.

3   In the Available Fields list on the left, select Locale.

4   Place the cursor in the Current Configuration list on the right where you want to insert the Locale field.

5   Click the **Plus** icon.

6   Click **Save**.

This personalization is stored in the database and therefore future patch deployments will not overwrite this (one-time) customization.

Editing existing translation strings files

You can make edits, additions, and deletions to string files 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.

1   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"
```

2   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"
```

3   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 string 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 the section Translating Get-Answers on page 142.

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.

Note: Peregrine recommends using the default setting, UTF-8, as UTF-8 encoding supports all of the other character sets available.

Character Encoding	Character Set
UTF-8	Supports all of the other encoding available.
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 Peregrine Portal** 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 display, or add, change, or delete records from a back-end database.

This section includes:

- Personalization overview on page 147
- Supporting personalization on page 156
- Personalization tasks on page 160
- Moving personalizations to a production environment on page 165

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. 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. DocExplorer 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 only appears on forms that allow personalization. The Personalization form determines what options appear in the Personalization pop-up window.

Note: The graphics used in this section are intended as examples only of the personalization options available on different forms and may not match exactly the options available for your application.

When you click on the Personalization icon, a pop-up window opens showing 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.

Administrators determine what available data fields display on each form. The Personalization form determines what options display in the Personalization pop-up window.

The form Personalization pop-up windows have the following format.

Field	Description
Available Fields	Shows all the document fields and sub-document 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. The $$IDS provides a lookup function that assoociates string variables with strings in a particular language. The file and instruction text is found in a language-specific file under the WEB-INF\apps directory.

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.

Adding and removing personalizations

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.

Choose a row in the Available Fields list and use the appropriate icon below to add or insert an element:

Icon	Description
	The Plus (+) icon adds a component to your current configuration.
	The Insert icon adds a component in the specified place on the screen.

Choose a row in the Current Configuration list and use the appropriate icon below to customize the form layout:

Icon	Description
	The Personalize (wrench) icon allows you to edit any attributes available for the field. The personalization options available depend on the type of element selected.
	See the following sections for more information: Configuring fields on page 152; Configuring subdocuments on page 153; and Configuring collections on page 155.
	The Move (vertical arrows) icons move the component either up or down on the page. Moving components is always performed with these arrows.
	The Remove (X) icon removes the component from the page.
	Removing a component does not delete the component; it only does not display it.

The Available Fields list also includes positioning features that allow you to group date on the form layout:

Icon	Description
-- Left/Right Split --	Create verticle columns at the insertion point.
-- Top/Bottom Split --	Create horizontal splits between fields at the insertion point.
--Section Title --	Create an editable section title name for a group of fields.

Configuring fields

After you select a field in the Current Configuration list, click the wrench icon to configure the field's attributes:

See the section Configuring field attributes on page 162 for more information about specific tasks. Depending on your personalization rights, you can rename the field label (see page 162), change the field to read-only (see page 163), require users to enter a value (see page 163), and change the size and span of a field (see page 164).

Configuring subdocuments

 Select a subdocument in the Current Configuration list and click the wrench icon to configure the subdocument.

Note: The Current Configuration list displays both fields and subdocuments. Not all forms include a subdocument.

When you personalize subdocuments, you have different Explorer Options than with higher-level interfaces.

Subdocuments that can be personalized contain the same icons as higher-level interfaces, including the wrench icon. However, subdocuments offer slightly different options.

Field	Description
Available Fields	Shows all the document columns that can be added to the current form. Peregrine OAA generates the list of available columns 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 columns are displayed in the form.
Current Configuration	Shows the document columns 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
    Lookup
    Popup
    Readonly
    Clear
    Required
    Exclude Drilldown
    Lookup Label
    Popup height
    Popup width
	Defines how Peregrine OAA displays results. Users see the Explorer Options section only if they have administrative Personalization rights.

Save	Saves and applies your Personalization changes to the current form.

Note: The first field for a subdocument is always used by the lookup to display the returned value from the lookup activity. If you do not want the lookup icon and link to appear at all, unchecked Lookup, clear all check box options, and clear the Label field for this subdocument. The remaining fields specified on the subdocument personalization form appear as fields on the current form. If Readonly is checked for the subdocument, then the fields are displayed as read-only.

Configuring collections

After you select a collection in the Current Configuration list, click the wrench icon to configure the collection.

When you personalize collections, you have different Explorer Options than with higher-level interfaces.

Collections that can be personalized contain the same icons as higher-level interfaces, including the wrench icon. However, collections offer slightly different options.

Field	Description
Available Fields	Shows all the document columns that can be added to the current form. Peregrine OAA generates the list of available columns 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 columns are displayed in the form.
Current Configuration	Shows the document columns and displays components that are on the current form.

Field	Description
Explorer Options Lookup Create Popup Remove Max. Row count More page row count Label Popup height Popup width	Defines how Peregrine OAA displays results. Users see the Explorer Options section only if they have administrative Personalization rights.
Save	Saves and applies your Personalization changes to the current form.

Note: A collection is handled as a many-to-many relationship if the first column of the collection is from another document. When personalizing a collection where you do not want a many-to-many relationship, make sure that its first column is not a subdocument reference; the first column in the collection must be a local attribute of the collected schema.

Supporting personalization

To support Personalization, you must have these components:

■ An AssetCenter, ServiceCenter or Rome 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 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.
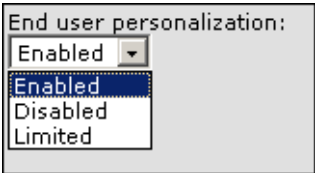
Personalization level	Description
Enabled	This setting grants all users the `getit.personalization.default` capability word, which enables end-users to add or remove any field listed in the schema used by a DocExplorer. However, only end-users who also have the `getit.personalization.admin` (or equivalent) capability word are 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 is hidden from the Get-Answers interface, and any end-users who have individual personalization rights 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-Answersback-end database. The following personalization capabilities words are available:

Capability word	Description
`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. Any changes this user makes are global. 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.

Note: The user that has the capability word **getit.portaladmin** creates the default portal page for all users that do not also have the **getit.portaladmin** capability word. There is one exception, however. The user "Admin", despite not having the **getit.portaladmin** capability word functions as if it does and can change the default portal settings as well.

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 provided personalization is available for the form. 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 appears 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 162 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.

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
Column span	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.
Row span	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 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 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.

Note: The import/export for personalization is only available to users having both `getit.admin` and `getit.personalization.admin` capability words.

To export personalization files:

1   Log in to the development application server.

2   Click **Administration** > **Import/Export** on the Administration tab.

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.

2   Click **Administration** > **Import/Export** on the Administration tab.

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

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

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.

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 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 195.

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 that lists 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 customizing 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 customizations.

Sample schema

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

Logical mappings

The file `\schema\extensions\rKmDocument.xml` lists the schema extension logical mappings. Logical mappings always use `name="base"`. The document name determines the schema name. This schema is `rKmDocument.xml`.

```
<?xml version="1.0" encoding="UTF-8"?>
<schema>
    <documents name="base">
        <document name="rKmDocument">
            <attribute label="Product" name="Product" type="string"
usertype="jsp:rtf_field.jsp"/>
            <attribute label="SubTitle" name="SubTitle" type="string"/>
            <attribute label="AuthorName" name="AuthorName"
type="string"/>
        </document>
    </documents>
</schema>
```

Physical mappings

The file `\schema\extensions\rome\rKmDocument.xml` lists the schema extension for the physical mappings. Physical mappings always use the adapter

name, for example, `name="rome"`. The document name determines the schema name. This schema is `rKmDocument.xml`.

```xml
<?xml version="1.0" encoding="UTF-8"?>
<schema>
    <documents name="rome">
        <document name="rKmDocument">
            <attribute field="_null" member="Product" name="Product"/>
            <attribute field="_null" member="SubTitle" name="SubTitle"/>
            <attribute field="_null" member="AuthorName"
name="AuthorName"/>
        </document>
    </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 customization tasks:

- 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 in:

`C:\<app_server>\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 12, 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 logical schema extension is located in the following subfolder on a typical installation:

`C:\<app_server>\webapps\oaa\WEB-INF\apps\oaagen\schema\extensions`

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

`C:\<app_server>\webapps\oaa\WEB-INF\apps\oaagen\schema\extensions\rome`

Each directory has an `rKmDocument.xml` file.

To create the schema extension target folders and files yourself:

Copy the sample schema rKmDocument.xml files from the previous section, Sample schema on page 169 into the two following directories.

Logical:

`C:\<app_server>\webapps\oaa\WEB-INF\apps\oaagen\schema\extensions`

Physical:

`C:\<app_server>\webapps\oaa\WEB-INF\apps\oaagen\schema\extensions\rome`

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 172.
- Hiding an existing field from the Available Fields list on page 173.
- Changing the label a field displays in the Available Fields list on page 174.
- Changing the list of forms where a field is available or visible on page 175.
- Changing the physical mapping of a field on page 176.
- Schema Elements and Attributes on page 195.

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 logical schema extension file in the `extensions` folder.

    This file is for your logical schema extensions.

2   In the logical file, 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:

```
<documents name="base">
  <document name="rKmDocument">
    <attribute label="Version" name="Version" type="number"/>
    <attribute label="Product" name="Product" type="string"
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 `Product` field above is an example of this.

Refer to <attribute> on page 199 for additional information on the `<attribute>` element.

3   Save the logical file.

4   Open the physical schema extension file in the `extensions\rome` folder.

    This file is for your physical schema extensions.

5   For each logical attribute that you added to the logical file, add an
    `<attribute>` element between the `<document>` tags for the physical
    attribute in the physical file.

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

a   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.

b   Add any optional attributes you want to use for the physical mapping.

See <attribute> on page 199 for more information on optional attributes of
the `<attribute>` element.

6   Save the physical 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:

1   Open the logical schema extension file in the `extensions` folder.

2   Locate the logical mapping for the field you want to remove.

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"` or
`name="Contact"`.

3   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="base">
  <document name="rKmDocument">
    <attribute name="Contact" label="Contact" search="false"
    list="false" detail="false" create="false" />
  </document>
</documents><documents name="base">
```

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

4   Save the logical 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 logical schema extension file in the `extensions` folder.

2   Locate the logical mapping for the field you want to change.

    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"` or `name="Contact"`.

3   Change the label attribute to the new desired value.

```
<documents name="base">
  <document name="rKmDocument">
    <attribute name="Contact" type="string" label="Representative"/>
  </document>
</documents>
```

4   Save the logical 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 logical schema extension file in the `extensions` folder.

2   Locate the logical mapping 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	search= search =true	search=true	search=false
Reports	list	list= list=true	list=true	list=false
Workflows and Reports	detail	detail= detail=true	detail=true	detail=false
Contribute New Document	create	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="base">
  <document name="rKmDocument">
    <attribute name="Contact" type="string" label="Contact"
     search="true" list="true" detail="true" create="true" />
  </document>
</documents>
```

4   Save the logical schema extension file.

Changing the physical mapping of a field

You can change the physical mapping that a field uses to point to another table or physical field.

To change the physical mapping of a field:

1   Open the rKmDocument.xml physical schema extension file in the extensions\rome folder.

2   Locate and change the physical mapping `<attribute>` element to match the new physical mapping you want.

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

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 199 for more information on optional attributes of the `<attribute>` element.

3   Save the physical schema extension file.

Sample schema extensions for Get-Answers

This section describes extending schemas for the documents (rKmDocument.xml), for hit highlighting and indexing, and for advanced searches.

Extend the rKmDocument schema

This section describes how to extend the rKmDocument.xml schema used by Get-Answers.

The default location for the file is

```
C:\<app_server>\webapps
\oaa\WEB-INF\apps\oaagen\schema\extensions\rKmDocument.xml
```

This file defines a sample logical schema extension mapping for rKmDocument.

```xml
<?xml version="1.0" encoding="UTF-8"?>
<schema xml:space="preserve">
    <documents name="base">
        <document name="rKmDocument" >
            <attribute label="Group" name="Group" type="string"/>
            <attribute label="Product_Class" name="Product_Class" type="string"/>
            <attribute label="Operating_System" name="Operating_System"
type="string"/>
            <attribute label="Creation_Date" name="Creation_Date" type="string"/>
            <attribute label="Last_Modified" name="Last_Modified" type="string"/>
            <attribute label="Priority" name="Priority" type="string"/>
            <attribute label="Problem" name="Problem" type="string"
usertype="jsp:rtf_field.jsp"/>
            <attribute label="Solution" name="Solution" type="string"
usertype="jsp:rtf_field.jsp"/>
            <attribute label="AuthorName" name="AuthorName" type="string"/>
            <attribute label="KnowlixDocument_ID" name="KnowlixDocument_ID"
type="string"/>
            <attribute label="History" name="History" type="string"/>
            <attribute label="JumpDestination" name="JumpDestination"
type="string"/>
            <attribute label="OwnedDocs" name="OwnedDocs" type="string"/>
        </document>
    </documents>
</schema>
```

In this example, the Problem and Solution fields have the attribute:

```
usertype="jsp:rtf_field.jsp"
```

This indicates that the data stored in this field will be Rich Text formatted. The Get-Answers application displays these fields using the Rich Text editor on the Contribute New Document page and the Workflow page.

Note: This applies only to the rKmDocument schema.

The default location for the file that defines the physical schema extension mapping for rKmDocument is:

```
C:\<app_server>\webapps
\oaa\WEB-INF\apps\oaagen\schema\extensions\rome\rKmDocument.xml
```

The following shows an example of the physical schema extension mapping for rKmDocument.

```xml
<?xml version="1.0" encoding="UTF-8"?>
<schema>
    <documents name="rome">
        <document name="rKmDocument" >
            <attribute field="_null" member="Group" name="Group"/>
            <attribute field="_null" member="Product_Class" name="Product_Class"/>
            <attribute field="_null" member="Operating_System"
              name="Operating_System"/>
            <attribute field="_null" member="Creation_Date" name="Creation_Date"/>
            <attribute field="_null" member="Last_Modified" name="Last_Modified"/>
            <attribute field="_null" member="Priority" name="Priority"/>
            <attribute field="_null" member="Problem" name="Problem"/>
            <attribute field="_null" member="Solution" name="Solution"/>
            <attribute length="30" field="KNOWLIXAUTHOR" member="AuthorName"
              name="AuthorName"/>
            <attribute field="_null" member="KnowlixDocument_ID"
              name="KnowlixDocument_ID"/>
            <attribute field="_null" member="History" name="History"/>
            <attribute field="_null" member="JumpDestination"
              name="JumpDestination"/>
            <attribute field="_null" member="OwnedDocs" name="OwnedDocs"/>
        </document>
    </documents>
</schema>
```

In this example, most of the fields appear as `field="_null"`.

When a field is mapped as `field="_null"`, this indicates that there is no physical mapping for this field. Fields without a physical mapping are packaged and stored in the DocBody blob field. All Rich Text fields must be stored in the DocBody blob field.

Note: Fields stored in the DocBody blob are not available for reporting.

If a field contains meta-data about the document that is necessary for reporting, it must have a physical mapping. In other words, the field must be mapped to its own column in the KMDOCUMENT table in the database. The `AuthorName` field in the example above has a physical mapping to the KNOWLIXAUTHOR column in the KMDOCUMENT table in the database, which indicates that the KNOWLIXAUTHOR column was added to the KMDOCUMENT table.

In order to specify a physical mapping for a field, the column being mapped to must exist in the database table. This can be accomplished using your database administration tool or it can be added as a new field in the BizDoc Table file

corresponding to the schema. In our example, the KNOWLIXAUTHOR field can be added to the file, Document.tbl. The default location is:

```
C:\<app_server>\webapps\oaa\WEB-INF\bizdoc\tables\KmDocument.tbl
```

The following shows an example of this file.

```xml
<?xml version="1.0" encoding="UTF-8"?>
<Tables>
    <Table name="KmDocument">
        <SuperClass/>
        <SqlName>KmDocument</SqlName>
        <LinkField/>
        <UniqueField/>
        <Fields>
            <Field name="Attachments">
                <Type>STRING</Type>
                <Length>1024</Length>
                <MappingType>DIRECTFIELD</MappingType>
                <SqlName>Attachments</SqlName>
                <DefaultValue/>
            </Field>
            <Field name="Component">
                <Type>STRING</Type>
                <Length>40</Length>
                <MappingType>DIRECTFIELD</MappingType>
                <SqlName>Component</SqlName>
                <DefaultValue/>
            </Field>

….

            <Field name="AuthorName">
                <Type>STRING</Type>
                <Length>30</Length>
                <MappingType>DIRECTFIELD</MappingType>
                <SqlName>KNOWLIXAUTHOR</SqlName>
                <DefaultValue/>
            </Field>
        </Fields>
        <Indexes/>
    </Table>
</Tables>
```

After the field is added to the KMDocument.tbl file, you must run the Create Tables process (Table Create) from the Peregrine Portal Administration page.

After the Create Tables process completes, you must restart the application server.

Indexing and hit highlighting extended fields

Once you have verified your extensions, you will need to perform a few more steps to make the Search engine aware of them. There are two different methods to accomplish this, based on whether the field is "_null" mapped or not. A "_null" mapped field is the simplest to work with.

You only have to create a field definition in the `rware.cfg` file on the Get-Answers Search engine server for each new field. If you have imported xml files, the document import tool creates a file containing default field mappings that you may cut and paste into your `RWare.cfg` file. This file is located at:

```
C:\<app_server>
\webapps\oaa\WEB-INF\apps\oaagen\schema\extensions\rware_cfg.txt.
```

Do not add a definition for any field you do not want to make searchable.

Note: The document importer does NOT create a sample field definition for fields already found in the schema, including new extended schema fields.

For fields with a physical mapping to a field in the KMDocument table of the database, you will need to perform a few extra steps. The first step is to create a field definition in `rware.cfg` for the field just like the "_null" mapped fields, but you have to manually create the field definition since the document importer will not generate a sample for you. The next step is to alter the SQL select statements in the `rware.cfg` file to select your new field for indexing. The default location of the `rware.cfg` file is `C:\getanswers\Peregrine\config` on your search engine server.

1   Start by making a backup copy of your current `rware.cfg` to a safe location.

2   Open rware.cfg in a text editor and search for

```
"/* >>>>> Functions for KMDOCUMENT */"
```

The SQL statements you need to modify are just below this marker.

3 The first function you modify is:

```
SELECT_ALL_DOCUMENTS FOR_LIBRARY KMLib.
```

4 The format of the SQL statements for `rware.cfg` is as follows:

- Function title, for example, `SELECT_ALL_DOCUMENTS FOR_LIBRARY KMLib`
- RWare field names enclosed in brackets`[]`.

Note: Pay special attention to the quotes around each line and the commas separating the names.

- The actual `"Select"` statement.

Note: When adding fields to the select statement, their order must match the order of the RWare fields in the brackets `[]`. The number of fields selected must also match the number of RWare fields in the brackets `[]`.

Example:

```
To add Version, change
  SELECT_ALL_DOCUMENTS FOR_LIBRARY KMLib
  "[title, rdb_primary_key, filename, docTitle, summary, "
  :
  :
  "LAUTHORID, FUNCTION SELECT_AuthorName, FUNCTION
SELECT_Category]"
  "SELECT TITLE,"
"        CONVERT(VARCHAR, LKMDOCUMENTID),"
  :
  :

to
  SELECT_ALL_DOCUMENTS FOR_LIBRARY KMLib
  "[title, Version, rdb_primary_key, filename, docTitle, summary,
"
  :
  :
  "LAUTHORID, FUNCTION SELECT_AuthorName, FUNCTION
SELECT_Category]"
  "SELECT TITLE,"
" Version,"
"        CONVERT(VARCHAR, LKMDOCUMENTID),"
  :
  :
```

5   Now add the RWare field name to the brackets [] section and the
     corresponding RDB field name to the Select statement. Repeat for all new
     fields you want indexed. Repeat steps 4 and 5 for the following functions:

     `SELECT_DOCUMENT_INSERTS FOR_LIBRARY KMLib,`

     `SELECT_DOCUMENT_UPDATES FOR_LIBRARY KMLib,`

     `AFM_GET_DOC_FIELDS FOR_LIBRARY KMLib.`

Note: Two of the select statements use joins. Prepend your RDB field name with
       `"P."`. Your fields should look like the others when done.

6   Save and close `rware.cfg`.

After modifying `rware.cfg`, you need to clear the Get-Answers search engine
indexes and reindex; otherwise, you get an error stating that the number of
bytes in the database do not match the index. Use the system utilities menu on
the Get-Answers search engine server to drop the indexes and perform a full
reindex of KMLib.

To drop the indexes and reindex KMLib:

1   From the Start menu, choose **Programs >Get-Answers Search
     Engine>Stop Search Engine Server**.

     The following messages appear:

     exec at IPAddress:port

     exec - shutdown

     Shutting down the Search Engine Server

     Press any key to continue . . .

2   Press any key to continue.

3   From the Start menu, choose **Programs> Get-Answers Search
     Engine>System Utilities Menu**.

4   Choose option 6 - **Indexing and index utilitie**s.

5   Choose option 11 - **Delete and create empty indexes for a library**.

6   At the "Indexes should be deleted for which library? Enter Library Name []>"command prompt, type **KMLib.**

7   At the "Are you sure? (1 = YES, 2 = NO)" command prompt, type *1*.

     These messages appear:

     Opening Library: KMLib

     Thank you!

8   Press any key to continue.

9   Choose option 1 - Return to previous menu.

10   Choose option 1 - Exit this program.

11   From the Start menu, choose **Programs> Get-Answers Search Engine**>**Start Search Engine Server**.

     These messages appear:

     Starting up the Search Engine Server

     Press any key to continue . . .

12   From the Start menu, choose **Programs > Get-Answers Search Engine >Reindex all Documents**.

13   At the "Enter the name of the library to be indexed. Enter Library Name []>"command prompt, type KMLib.

14 At the "Are you sure you wish to index the entire RDBMS now? (warning: this will delete any existing indexes in KMLib). (1 = YES, 2 = NO)" command prompt, type **1**.

This message appears:

All records have been submitted to the document handler.

15 Press any key to continue.

The new fields are now indexed and searchable. See for an explanation of how to make your fields available from the advanced search screen.

If you wish to have hit highlighting applied to your RDB fields, perform the following:

1 Make a backup copy of `C:\getanswers\Peregrine\dp\KMLib.dp`.

2 Open `KMLib.dp` with a text editor and search for: `SGML_SUB XML_PARSER_VIEW`.

3 Just below the embedded comments, you will see a series of `"VIEW LITERAL"` statements. Simply copy one of the un-commented lines and paste it at the end of the list.

4 Change previous field name to the name of your new field.

Note: There are four occurrences of the field name in each statement to be changed. Repeat for all fields you wish to hit highlight.

Extending advanced search

If you wish to make new fields available on the Advanced Search screen, you must extend the kmSearchFields schema. The default location for this file is:

```
C:\<app_server>\webapps\oaa\WEB-INF\apps\getanswers\schema
```

Use the guidelines describe in to extend this schema.

There are three important conditions that must be met when extending the kmSearchFields schema.

- All fields MUST be mapped to _null in the physical extension mapping file.
- All fields MUST be defined in the LIBRARY "KMLib" section of the `rware.cfg` file in the Get-Answers Search Engine. The default location for this file is in the config folder, `C:\getanswers\Peregrine\config`.
- All field names MUST match the UF_NAME defined for that field in the `rware.cfg` file.

The followings shows an example of this code.

```
LIBRARY "KMLib" {

…

    FIELD "AuthorName" {
      INFO "Author Name.";
      UF_NAME "AuthorName";
      PRECEDENCE 1;
      SIZE 30;
      TYPE STRING;
      FLAGS STORED INDEXED VISIBLE NATURAL_LANGUAGE USER_SEARCH
WITH_BODY BOOLEAN_ONLY RESULTS_LIST;
    }

…
```

Sample schema extension for document feedback form

This section provides an example of how you would personalize a document feedback form by adding additional fields to the form. In this example, you will be adding two fields to the feedback form, Summary (FeedbackSummary) and Correct.

Document Details

Title:	Baseball
Summary:	Baseball is very, very good to me.

Editorial Status:	Published	**Date Document Last Modified:**	9/9/04
Creation Date:	9/9/04	**Expiration Date:**	9/9/05

Feedback

Summary: [   ]

Comments: [   ]

Was this document useful to you?

○ Yes
○ No

Was it correct?

○ Yes
○ No

[Submit] [Close]

To personalize the document feedback form:

1   Add the fields to
    *<deployment_dir>***\WEB-INF\bizdoc\tables\KmDocumentFeedbacks.tbl**.

    The following shows a sample of the code added to the
    KmDocumentFeedbacks.tbl file.

```xml
<?xml version="1.0" encoding="UTF-8"?>
<Tables>
    <Table name="KmDocumentFeedbacks">
        <SuperClass/>
        <SqlName>KmDocumentFeedbacks</SqlName>
        <LinkField/>
        <UniqueField/>
        <Fields>
            <Field name="FeedbackDate">
                <Type>DATE</Type>
                <Length>30</Length>
                <MappingType>DIRECTFIELD</MappingType>
                <SqlName>FeedbackDate</SqlName>
                <DefaultValue/>
            </Field>
...
<!-- Example: added the following two fields, one is a text
field, the other is essentially a boolean -->
            <Field name="FeedbackSummary">
                <Type>STRING</Type>
                <Length>200</Length>
                <MappingType>DIRECTFIELD</MappingType>
                <SqlName>FeedbackSummary</SqlName>
                <DefaultValue/>
            </Field>
            <Field name="Correct">
                <Type>STRING</Type>
                <Length>30</Length>
                <MappingType>DIRECTFIELD</MappingType>
                <SqlName>Correct</SqlName>
                <DefaultValue/>
            </Field>

        </Fields>
        <Indexes/>
    </Table>
</Tables>
```

2   Add the fields to
     <deployment_dir>**WEB-INF\apps\oaagen\schema\KmDocumentFeedba
     cks.xml**.

The following shows a sample of the code added to the
KmDocumentFeedbacks.xml file**.**

```
 <schema>
            <documents name="base">
                <document version="1.0" UniqueField="" extends=""
name="rKmDocumentFeedbacks"
label="$$IDS(Entities,Entities_KmDocumentFeedbacks_Label)"
loadscript="loadscript.rKmDocumentFeedbacks.kmDocumentFeedbacksLo
adScript">
                    <attribute access="r" ACLlist="OAA.admin"
ACLdetail="OAA.admin" ACLsearch="OAA.admin" ACLupdate="OAA.admin"
ACLcreate="OAA.admin" type="id" label="$$IDS(bizdoc,LabelId)"
name="Id"/>
...
<!-- Example: added the following two fields here too -->
                    <attribute callmethod="" length="200"
field="FEEDBACKSUMMARY" member="FeedbackSummary"
name="FeedbackSummary"/>
                    <attribute callmethod="" length="30"
field="CORRECT" member="Correct" name="Correct"/>

                    <document displayfield="KmDocument_I_String"
joinvalue="KmDocument_I_Id" joinfield="LKMDOCUMENTID"
type="NORMAL" name="KmDocument"/>
                    <document displayfield="User_I_String"
joinvalue="User_I_Id" joinfield="LTBLPERSONID" type="NORMAL"
name="User"/>
                </document>
            </documents>
        </schema>
```

3 Add text strings for labels to
<deployment_dir>**WEB-INF\apps\oaagen\Entities_en.txt** (and files) to
match label entries in the base section of *rKmDocumentFeedbacks.xml*.

The following shows a sample of the code added to the *Entities_en.str* file**.**

```
;#**************************************************
;#  'Entities' multilingual strings
;#**************************************************
;#
;#  Language: en
;#  All multilingual properties (ending with '_en')
;#  International build: true
;#  Encoding: ISO-8859-1
;#
;#**************************************************

Entities_KmAttachment_Label, "Attachment"
Entities_KmAttachment_Members_Content_Label, "Content"
Entities_KmAttachment_Members_Description_Label, "Description"
Entities_KmAttachment_Members_LegacyId_Label, "Legacy Id"
Entities_KmAttachment_Members_Parent_Label, "Document Ownership
Team"
...
;# Example: added the following two strings to match the labels
used in rKMDocumentFeedbacks.xml
Entities_KmDocumentFeedbacks_Members_FeedbackSummary_Label,
"Summary"
Entities_KmDocumentFeedbacks_Members_Correct_Label, "Correct"
...
Entities_rwu_KmDocument_Members_action_Label, "Action"
Entities_rwu_KmDocument_Members_LKMDOCUMENTIDSTR_Label,
"KmDocument Id String
```

4   If the field you add is a special file such as a drop-down list, create the jsp in *<deployment_dir>*.

The following shows a sample of the code added to *ga_correctfield.jsp*.

```
/* Example: Changed this file (after copying the useful select
field jsp) for the purpose of
        having a new yes/no radio button in the survey */

<%@ include file="componentheader.jsp" %>
   ...
/* DJM: i changed the value of the parameter from Useful to
Correct */
        String strRadioField = msgModel.get("Correct");

      //display strRadioField as static text on form
      if(strRadioField.equals("true"))
        strRadioField = IDS.get(cw.getUser().getLocale(),
"getanswers","Yes");
      else if(strRadioField.equals("false"))
        strRadioField = IDS.get(cw.getUser().getLocale(),
"getanswers","No");
      else if(strRadioField.length() < 1)
       strRadioField = "";
      cw.out.println( strRadioField );
      }
     else //This is the code that is called when we are Authoring
the document
      {
       // This does not display normally, but is used for section
508 compliance.
/* Example: Changed the value of the strTitle from UsefulField to
CorrectField */
        String strTitle = "CorrectField";
...

/* Example: Changed the value of the parameter name and id from
        rKmDocumentFeedbacks_I_Useful to
rKmDocumentFeedbacks_I_Correct */
        cw.out.println("<BR><INPUT
name='rKmDocumentFeedbacks_I_Correct' type='radio'
id='rKmDocumentFeedbacks_I_Correct' value='false' title='Not
Correct'>" + IDS.get(cw.getUser().getLocale(), "getanswers","No")
+ "</INPUT>");

    }
  }
%>
```

5   If necessary, add other strings to
     <deployment_dir>**WEB-INF\apps\getanswers\getanswers_en.str**

     The following shows a sample of the code added to *getanswers_en.str*.

```
;#***************************************************
;#  'getanswers' multilingual strings
;#***************************************************
;#
;#  Language: en
;#  All multilingual properties (ending with '_en')
;#  International build: true
;#  Encoding: ISO-8859-1
;#
;#***************************************************

getanswers_answers_appmenutitle, "Get-Answers"
getanswers_answers_label, "Get-Answers"
getanswers_answers_kmSearchAlternate_label, "Search"
getanswers_answers_kmSearchAlternate_basicSearch_title, "Ask a
Question"
...
;# Example: Added the following string for the feedback form
InfoWasCorrect, "Was the information in this document correct?"
...
WSAttachPathInst, "The path to the knowledge documents within (or
from the point of view of) the web servers file management
system."
xslSkipToNavigationMenu, "Click Enter to tab to the Navigation
Menu"
Yes, "Yes"
```

6   Personalize the form for capturing feedback. See *Chapter 5, Personalization*
     for additional information.

7   Personalize the form for viewing feedback. See *Chapter 5, Personalization* for
     additional information.

8   Personalize the reports (query, list, and details) for feedback.

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.

```
<?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 atrribute 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`.

`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`.

Optional attributes

`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 attributes 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 atrribute 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 atrribute 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 atrribute 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 atrribute 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 `search="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 attributes 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.

Preserving custom SelectFields

In order to avoid customized selectfields (`ga_selectfield1.jsp` –
`ga_selectfield5.jsp`) from being overwritten during future upgrades, you can
use a schema extension to override the `SelectField1...SelectField5`
attributes in the rKmDocument schema. The usertype attribute indicates which
jsp file to use for displaying the field. Make a copy of the out-of-box `.jsp`
indicated for this field, then rename the file. You can then perform
customization on the renamed `.jsp` file. In the schema extension, you can
override the `SelectField` attribute and change the usertype attribute to point
to the new `.jsp` file.

Make a copy of `ga_selectfied1.jsp` located in `<TOMCAT_HOME>\webapps\oaa`
and rename it to `MYSELECTFIELD1.jsp`. Create a schema extension for
rKmDocument to override the out-of-box attribute for SelectField1:

```
<attributelabel=
    "$$IDS(Entities,Entities_KmDocument_Members_SelectField1_Label)"
    name="SelectField1" type="string"
    usertype="jsp:ga_selectfield1.jsp" localize="false" required="false"
    tokensleft="false"/>
```

and change it to:

```
<attributelabel=
    "$$IDS(Entities,Entities_KmDocument_Members_SelectField1_Label)"
    name="SelectField1"
    type="string" usertype="jsp:MYSELECTFIELD1.jsp" localize="false"
    required="false"
    tokensleft="false"/>
```

This ensures that future upgrades and patches do not overwrite the
customizations for these fields.

CHAPTER 7 | Get-Answers Administration

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

Topics in this chapter include:

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 on 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.

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:

```
http://<hostname>:<port>/oaa/admin.jsp
```

3   Press Enter to open the Portal administrator login page.
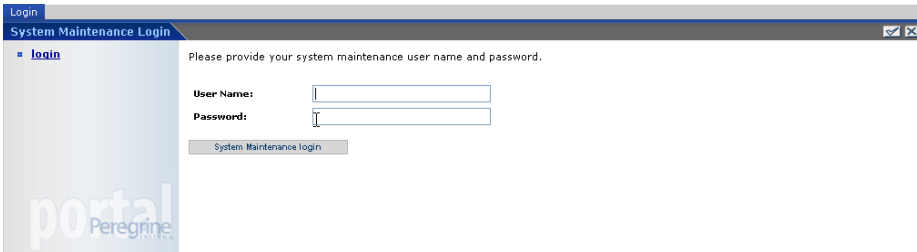
4   In the Name field, type **System**.

No password is required on initial login.

5   Click **System Maintenance login.**

6   Click **Control Panel** to open the Control Panel page.
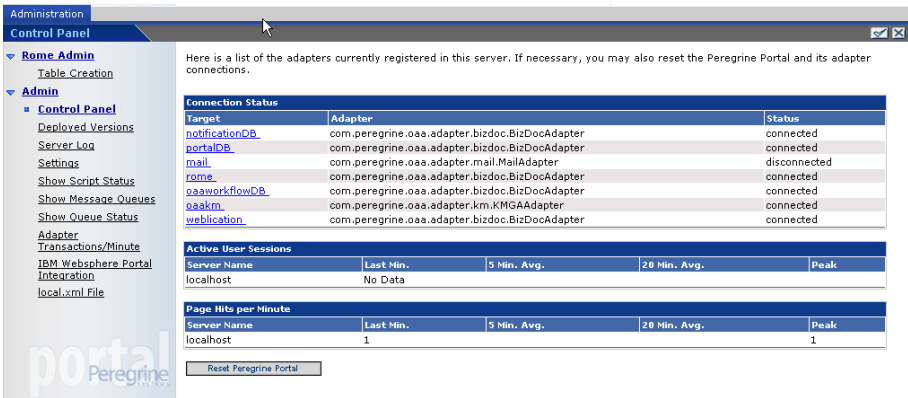
The activities available in the Admin module include:

Select this option	To do the following
Table Creation	Create database tables and populate them with Get-Answers sample data.
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.

Select this option	To do the following
Settings	View and change settings for the Peregrine Portal.
Show Script Status	View and verify which application 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.
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
local.xml File	Download the local.xml file

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 Peregrine Portal.**

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

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.

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

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. Use the E-mail tab to configure E-mail, so that users are notified by E-mail of their password when users have access to self-registration (see User self-registration on page 230).

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.

Setting parameters using the Admin module

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

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.

3   From the Activity menu, click **Control Panel > Reset Peregrine Portal**.

An information message at the top of the Control Panel indicates that the server has been reset.

Choosing a login language

When you log in to the Peregrine Portal, you can choose from the Language pull-down list the language that the Portal displays. The default language is English, but you can enable additional languages.

Note: You can only enable additional languages if the language packs are deployed.

To enable additional login languages:

1   Click **Settings** in the Control Panel.

2   Scroll down to the **Encoding**, **Locales**, and **Sessions** section.

3   In the Locales field type a comma-delimited list of the languages you want to enable.

The first locale defines the default; in this case **en** for English, which already appears in the field. A locale is specified by the ISO-639 language code, which you can combine with the ISO-3166 Country code, separated with an underline (_). For example, **fr** enables French; **en** and **en_US** specify U.S. English, where dates are formatted Month/Day/Year; **en_GB** specifies British English, where dates are formatted Day/Month/Year. The value

en_GB,fr,de,it specifies that British English, French, German, and Italian are enabled.

4   Make sure that **Yes** is specified for **Enable Logout**. This is important because you need to log out of the Peregrine Portal and log back in for your changes to take effect.

Logging

You can use the Logging tab in the Admin Settings page to customize the logging of events in a server log file, whose default name is `archway.log`. A sample list appears in the text describing the Log domain text box.

The valid debug domains include the following:

acadapter	AssetCenter adapter (authentication, authorization, and adapter services)
answers	The answers domain enables logging in the Get-Answers ECMA application scripts.
scadapter	ServiceCenter adapter (authentication, authorization, and adapter services)
mailadapter	used for email

bizdoc	The bizdoc domain enables logging in the bizdoc platform which is used by Get-Answers. This displays details of all queries edecuted by Get-Answers. There is also a setting in the Get-Answers admin page to enable adapter logging that displays logging information for the kmadapter.
trigger	schema object trigger subsystem
bizdocadapter	BizDoc adapter (authentication, authorization, and adapter services)
presentation	how personalizations are delivered
personalization	wrench icon
weblication	personalization operations
archway	Archway services
ProcessorFactory	OAA internal request handling system (script, database and administration)
AdminController	Administrative request handling object
security	JAAS login modules to authenticate users
statistics	fundamental OAA statistics (moving averages)
oaaworkflow	workflow processes
templateengine	workflow templates
notificationservices	periodic script pollers that check for workflow assignments and workflow-related email notifications

The Log Level parameter allows you to specify the level of detail for the log information written to the log file. The All setting captures the most detail and the other settings specify various degrees or types of information collected for the specified Log domains. Possible values are: all, debug, info, warn, error, fatal and off in reverse order of detail. Typically this setting should be left at warn or error so the logs indicate any significant problems encountered during production use. The more verbose settings of debug and info should be used during tailoring or problem isolation.

Note: You can also set logging parameters on the Rome tab and the Get-Answers tab. As you increase the log level detail, the archway.log dramatically increases in size. Please consult with Customer Support if you have questions regarding these features or their effects on your system.

Logging format

You can specify in the Logging Format field the printing pattern of a log file. The logging format is composed of literal text and conversion specifiers. The details of the specifiers can be found in the following table, which can be found in its entirety, along with additional information, on the Apache.org web site at: *http://logging.apache.org/log4j/docs/api/org/apache/log4j/PatternLayout.html*

Logging format table

Conversion character	Effect
c	Used to output the category of the logging event. The category conversion specifier can be optionally followed by *precision specifier*, which is a decimal constant in brackets.
	If a precision specifier is given, then only the corresponding number of right-most components of the category name will be printed. By default the category name is printed in full.
	For example, for the category name "a.b.c" the pattern %c{2} is output as "b.c".
C	Used to output the fully qualified class name of the caller issuing the logging request. This conversion specifier can be optionally followed by *precision specifier*, which is a decimal constant in brackets.
	If a precision specifier is given, then only the corresponding number of right most components of the class name will be printed. By default the class name is output in fully qualified form.
	For example, for the class name "org.apache.xyz.SomeClass", the pattern %C{1} is output as "SomeClass".
	Note: Generating the caller class information is slow. Avoid it unless execution speed is not an issue.
d	Used to output the date of the logging event. The date conversion specifier may be followed by a *date format specifier*, which is enclosed in braces, such as
	`%d{HH:mm:ss,SSS}`
	or
	`%d{dd MMM yyyy HH:mm:ss,SSS}`
	If no date format specifier is given then ISO8601 format is assumed.
F	Used to output the file name where the logging request was issued.
	Note: Generating caller location information is extremely slow. Avoid it unless execution speed is not an issue

Conversion character	Effect
l [lower-case letter]	Used to output location information of the caller that generated the logging event. The location information depends on the JVM implementation, but usually consists of the fully qualified name of the calling method followed by the caller's source, the file name, and the line number enclosed in parentheses. Note: Though location information can be very useful, its generation is *extremely* slow. Avoid it unless execution speed is not an issue.
L	Used to output the line number from where the logging request was issued. Note: Generating caller location information is extremely slow. Avoid it unless execution speed is not an issue.
m	Used to output the application supplied message associated with the logging event.
M	Used to output the method name where the logging request was issued. Note: Generating caller location information is extremely slow. Avoid it unless execution speed is not an issue.
n	Outputs the platform-dependent line separator character(s), which offer practically the same performance as using non-portable line separator strings such as "\n" or "\r\n". Thus, it is the preferred way of specifying a line separator.
p	Used to output the priority of the logging event.
r	Used to output the number of milliseconds elapsed between the time when the application started and the time of the logging event.
t	Used to output the name of the thread that generated the logging event.
x	Used to output the NDC (nested diagnostic context) associated with the thread that generated the logging event.
X	Used to output the MDC (mapped diagnostic context) associated with the thread that generated the logging event. The X conversion character *must* be followed by the key for the map placed between braces, as in: `%X{clientNumber}` where `clientNumber` is the key. The value in the MDC corresponding to the key will be output.
%	The sequence %% outputs a single percent sign.

The format of the log file is determined by the Apache PatternLayout class.

Log file rollover

You can specify in the Log File Rollover Frequency Pattern field the frequency with which the log file is rolled over. The pattern that you enter is also used as an extension to name non-active files. By default the log file rolls over at midnight on the first day of each week, and logs a maximum one week's data. However, you can specify that the log files roll over at the following intervals: monthly, weekly, half-daily, daily, hourly, or every minute. Use the parameters in the following table, which can be found in its entirety, along with additional information, on the Apache.org web site at *http://logging.apache.org/log4j/docs/api/org/apache/log4j/ DailyRollingFileAppender.html*

Date pattern	Rollover schedule
'.'yyyy-MM	The beginning of each month
'.'yyyy-ww	The first day of each week, depending on the locale
'.'yyyy-MM-dd	At midnight each day
'.'yyyy-MM-dd-a	At midnight and midday of each day
'.'yyyy-MM-dd-HH	At the top of every hour
'.'yyyy-MM-dd-HH-mm	At the beginning of every minute

The Apache DailyRollingFileAppender class determines the log file rollover frequency.

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.
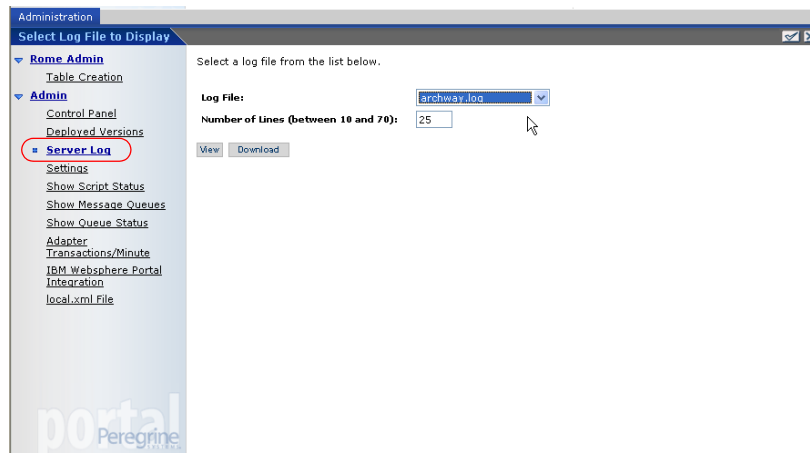
2 Click the drop-down and select the log file you want to view.

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.

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.
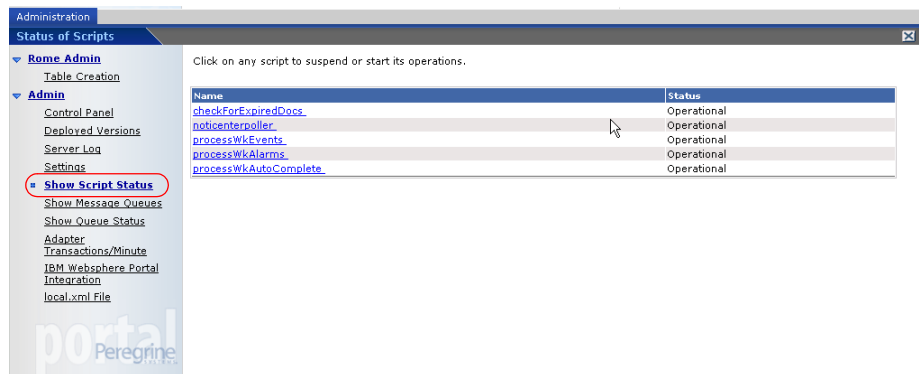
2 Click on the script to suspend it.

If the noticepoller, `processWkEvents`, `processWkAlarms`, or `processWkAutoComplete` scripts are suspended, workflow does not process workflow activities in Get-Answers.

Displaying Message Queues

The Message Queues display whenever a queue has data waiting to be transferred. Notification Services processes the messages in these queues every 20 seconds unless an error occurs. Ensure that under Show Script Status, the noticepoller, `processWkEvents`, `processWkAlarms`, `processWkAutoComplete` scripts are operational and not suspended.

To display message queues:

1 From the **Administration** Activity menu, click **Show Message Queues** to display the **Active Queues** page.
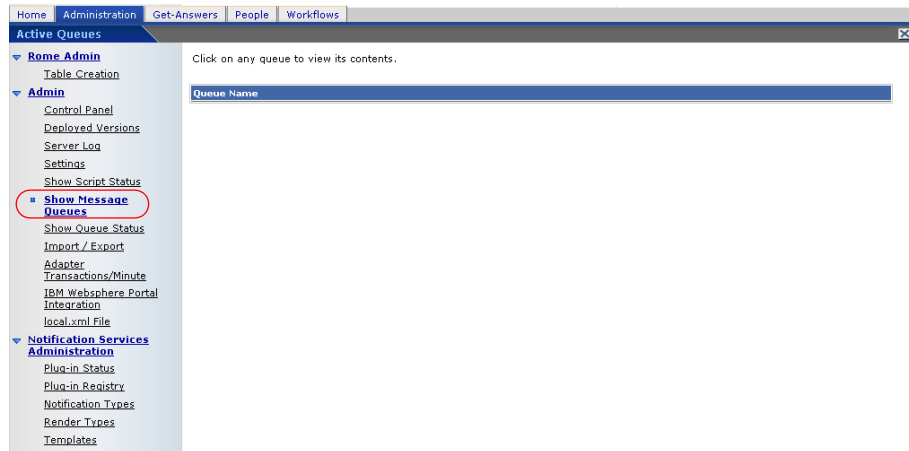
2 Click the queue name in the list to view the contents of a queue.

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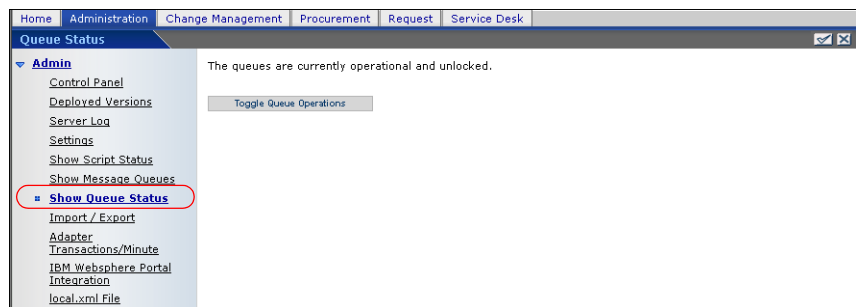
2   Click **Toggle Queue Operations** to change the status to **suspended**.

A warning message indicates that the Queue Status is suspended.
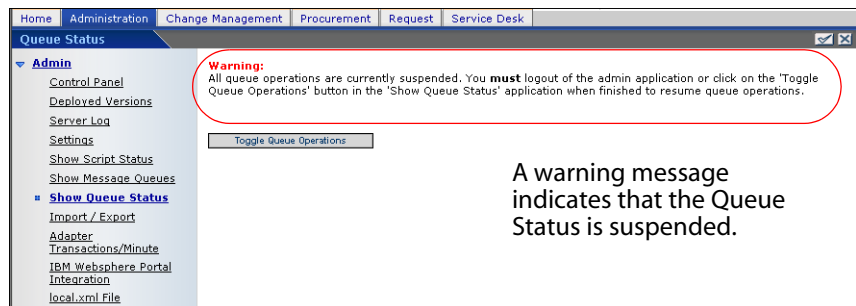
3   Click **Toggle Queue Operations** to return to the operational status.

Importing and exporting personalizations

You can move personalizations that you created in a development environment to a production environment. See the Personalization 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.
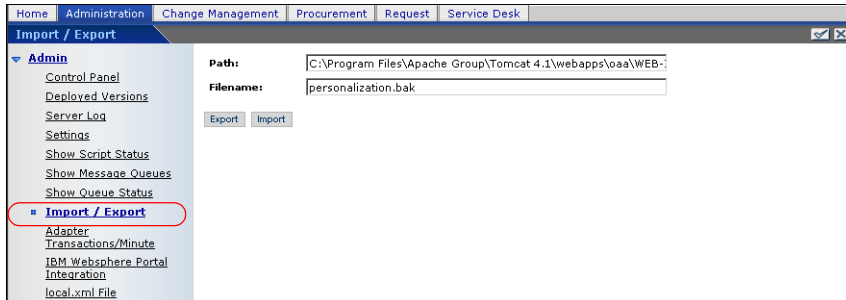
Viewing adapter transactions

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**.

Downloading the local.xml file

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. You can download the `local.xml`to preserve your settings if you want to test other settings and then replace the `local.xml` file your test created with your original `local.xml`.

To download the local.xml file:

1   From the Activity menu, click **local.xml File** to open the Download local.xml File page.

2   Click **Download**.

3   In the File Download dialog box, select **Open** or **Save**.

4   If you selected Save, specify the save location for the `local.xml` 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** > **Logging**.

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

3   Click **Save**.

4   For this particular setting, it is not necessary to Reset Peregrine Portal.
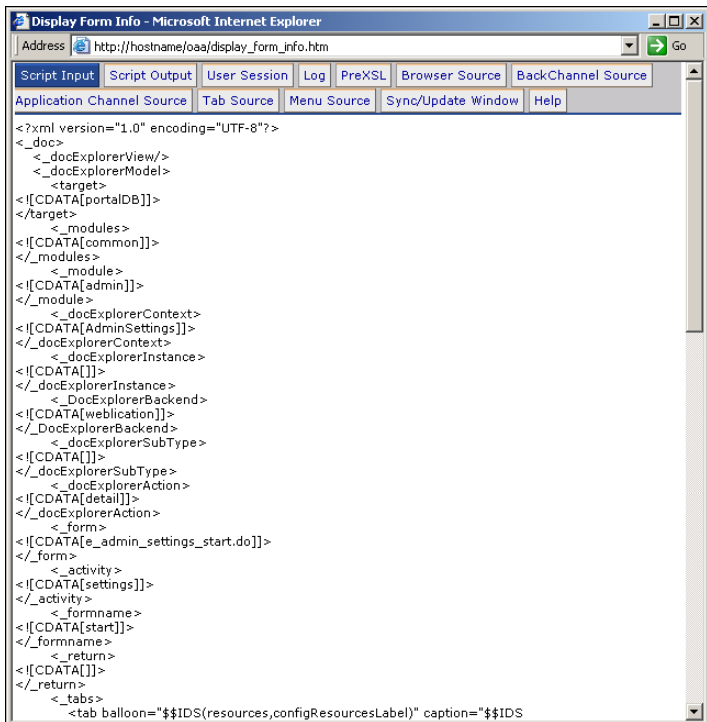
The name of the form is at the top of each form.

The form name is at
the top of the page.

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.

This is a partial example of the contents in the PortalDB tab.

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

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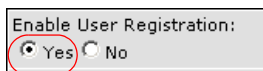
This tab	Contains
Application Channel Source	HTML source code for the shared applications.
Tab Source	HTML source code for tabs.
Menu Source	HTML source code for menus.
Sync/Update Window	HTML source code to synchronize with the page and reload.
Help	Help for debugging the window.

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 rome database. When the user registers, the system creates an RESSRC record and a TBLPERSON record for the new user with basic user login rights. See the Security chapter in this guide for more information about 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**.

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**.
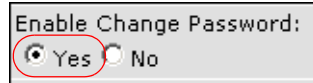
   Click Yes to give users the ability to change their own passwords.

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.

```
127.0.0.1 - Tossi [04/Oct/2004:12:17:25 -0700] "GET portal
/portal/main/e_login_main_process.do 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
127.0.0.1	-	Tossi	[04/Oct/ 2004:12:17 :25 -0700]	`"GET portal/portal /main/e_login_main_ process.do 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.
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.

Get-Answers tab

The Get-Answers tab displays the configuration settings for Get-Answers on a single page. On this page, you can reset any of the settings and then click Save at the bottom of the page to update the settings. This page is useful for viewing the current settings and quickly seeing settings that may be incorrect.

To access the Get-Answers tab:

1   Click **Settings** under the Admin Activity menu.

2   Click the **Get-Answers** tab.

The Get-Answers tab opens.

On this tab you can:

■   View or update many of the settings for the search engine.

■   Allow administrators to retire linked documents. If the Allow Retirement of Linked Documents is set to Yes, the Retire button appears on the Actions form of any linked document.

■   Allow administrators to determine whether or not working copies of documents should appear in knowledge searches. If the administrator selects the 'Yes' option for the Show Working Copies setting, working copy documents are included and displayed in the search hitlist for Owners, Editors, Reviewers, and Readers.

Managing linked documents

The Link Management Utility enables you to verify the document links specified in each published document. You can configure the utility to verify the links for the documents in a specific document ownership team or for all the document ownership teams. When your system contains a large number of documents, the process may take a considerable amount of time. The Link Management Utility reports on the number of links found, validated links, fixed links, broken links, converted 4.1.x links, total errors, and documents processed.

Note: The Link Management Utility does not verify external/HTML links such as http:// , ftp://, or file:// links to Web pages or sites found outside of Get-Answers.

To use the Link Management Utility:

1   Log in to Get-Answers.

2   Click the Get-Answers tab.

3   Click Reconcile Linked Documents in the Activity menu.

The configure page for the Link Management Utility opens.
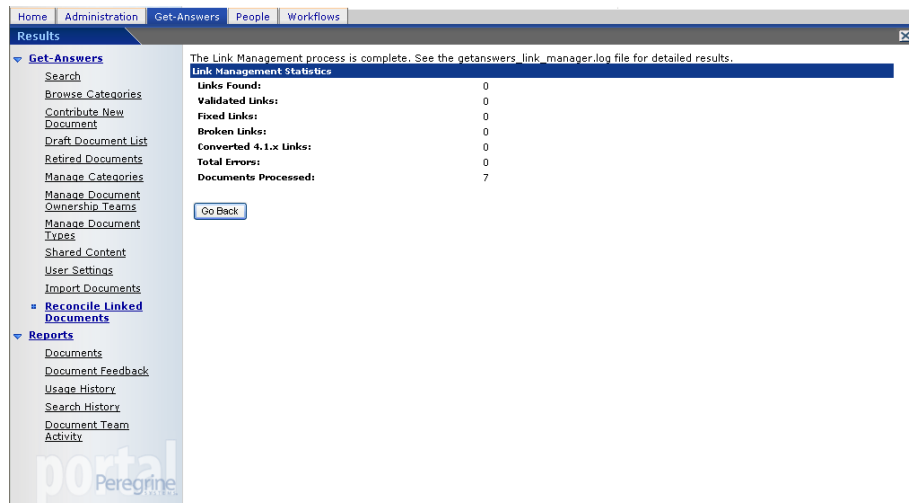
4   Select the document ownership team to process.

5   Click Run Link Management Utility.

When the utility completes processing all of the documents, the results
page opens.
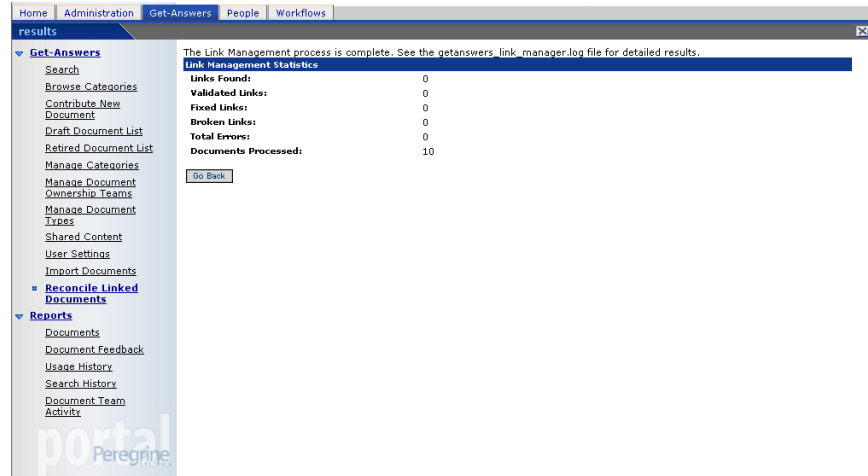
6   Review the results. You can also view the *getanswers_link_manager.log* file.
This file is in the webapps\oaa directory of where you installed Get-Answers.
For example, C:\Program Files\ Apache Group\Tomcat 4.1\webapps\oaa.

8

CHAPTER

Get-Answers Security

This chapter describes the different security configuration options available in Get-Answers. Topics in this chapter include, password and access rights for Health Insurance Portability and Accountability Act (HIPAA) support, default and custom security configurations, authentication, and alternate login pages.

By default, Get-Answers does not encode passwords sent over the network; however, passwords are stored in SHA-1 format (encrypted format) in the database. 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 Integrated Windows Authentication

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 247.

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 256.

Back-end system security

This section includes information about how Get-Answers authenticates users and stores personalization changes in the ServiceCenter, AssetCenter, or Rome back-end system.

User account and password management

This section describes how the Administrator can manage user accounts and setup password formatting rules.

General administrative options

There are administrative options that apply to all the back-end adapters. These options are listed on the Common tab of the Administration page.

Enable Change Password: The **Yes** option enables the display of the **Change Password** portal component for user accounts that are granted with the `getit.password` capability. The **No** option requires the administrator to change passwords for all users.

Allow current password to be new password: The **Yes** option gives administrators the ability to require users to enter a new password that is different from the current password when they are using the Change Password options.

Rome options using the People tab

Administrator can use the security options displayed on the detailed screen under the People tab to manage individual accounts.

All time values displayed in Pacific Standard Time time zone.

Document Details
Last Name: New   Login Name: password
First Name: User

Security
Login Password:
Account Disabled: ☐
Account Locked Out: ☐
Password Never Expires: ☑
Change Password On Next Login: ☐
Password Expiration Date: Jun ∨ 2 ∨ 2005 ∨ 4 ∨ : 18 PM ∨

Login Password: This can be used to set or reset the password for a user account.

Note: Updating this field always clears the "Change Password ON Next Login" check box and recalculates the value for the Password Expiration Date field.

Account Disabled: This prevents user from logging on to the system. User may also lose access to some of the Get-Answer and Workflow functions, such as getting Workflow messages.

Account Locked Out: When checked, this prevents a user from logging on to the system when a user fails to logon to the system within the maximum number of consecutive attempts. If the security option, "Account Lock-Out with Failed Password Resets" on the Admin Settings page (Rome tab) is set to "Yes," the system automatically checks this setting. The administrator can clear this setting to unlock the account so that the user can try to logon again.

Account Never Expires: When checked, this flag sets a flag on so that the "Change Password On Next Login" and "Password Expiration Date" settings are ignored.

Change Password On Next Login: When checked, sets a flag so that users are prompted to change password after the user successfully logs on to the system.

Note: If this check box is checked at the same time the Login Password is updated, the resulting update unchecks Change Password On Next Login.

Password Expiration Date: This field is automatically calculated and populated for a new user account using the values configured in the Security section on the Rome tab. The Administrator can override this calculated date.

Note: If this date is changed at the same time the Login Password is updated, the resulting update resets the value of the Password Expiration Date with the new calculated value.

Security options on the Rome tab

Administrator can use the options on the Rome tab (Admin Settings page) to specify rules that are applied to all users.

The values entered in the "Duration in which a login password is valid" and "Units for Duration of a valid login password" options are used to calculate the value for the "Password Expiration Date" field.

If the "Account Lock-out with Failed Logins" option is turned on (Yes), the values entered in the "Max Failed Login Attempts" are used to automatically lock out a user account if a user has reached the maximum number of consecutive attempts to logon to the system.

If the "Account Lock-out with Failed Password Resets" option is turned on (Yes), the values entered in the "Max Failed Password Reset Attempts" options is used to automatically lock out a user account if a user has reached the maximum number of consecutive attempts to logon to the system or reset the password.

Authentication with ServiceCenter or Rome

When a user logs on to Get-Answers, the user name and password are validated against a corresponding operator record in ServiceCenter. For Get-Answers, the user name and password are validated against a set of tables in the Rome database and according to the settings described in Rome options using the People tab and Security options on the Rome tab sections. Each record or employee profile must contain appropriate capability words or user-right keywords in order to gain access to various features within Get-Answers.

When a user logs on, the ServiceCenter or Rome back-end validates the user password, account status, and the password expiration according to the rules defined in each respective system. Rome checks these conditions in the user's account in the following order.

1 Account disabled

2 Account locked out

3 The password entered is correct

4 Password Never Expires setting

5 Change Password On Next Login setting

6 Password Expiration Date setting

A generic error appears when a user fails to authenticate to any of the back-ends.

```
Sorry, your password has expired in at least one of the
supported targets. Please reset your password before you enter
the Peregrine Portal.
```

More back-end specific errors may be available in the `archway.log` file.

When one adapter returns an expired password code, the system redirects the user to the Change Password screen. A generic error is used for password format error for the ServiceCenter back-end and this can be customized by modifying the value for the `changePasswordGenericError` property in the common language string file located under the `WEB-INF\apps\common` directory.

The user cannot log on to the system unless the user successfully resets the password.

Both the **Current Password** and **New Password** are sent to the back-end adapters. The ServiceCenter back-end is responsible for verifying the current password and making sure that the new password complies with the rules and format for the password.

Generic error messages are displayed when a user has failed to reset the password. These messages can be customized by modifying the properties in the portal language string file in order to specify password format restrictions if desired.

Specific error messages may be found in the `archway.log`.

Following is a list of available capability words and user rights keywords for Get-Answers functionality that can be assigned to a record in ServiceCenter or rome or a profile in AssetCenter.

Access	Description
ga.docteam.admin	Can modify ALL document ownership teams in order to assign an owner
ga.docteam.create	Can create a document ownership team
ga.docteam.delete	Can delete a document ownership team
ga.docteam.manage	Can assign an owner, editor, reviewer, or reader to any document ownership team in which the user is the owner
ga.document.edit	Can transfer, retire, or create an editorial workflow to modify a published document or modify a working copy document; can view feedback
ga.document.new	Can create an authored (rich text) document
ga.document.read	Necessary capability for the Get-Answers tab to appear, user needs this capability in order to search, or browse categories, or view Get-Answers Help
ga.document.submit_batch	Can submit one or more native documents to be immediately published to a domain category
ga.document.submit_draft	Can submit a new native document to be considered for publication by the document ownership team

Access	Description
ga.domain.create	Can create a domain (group of published documents)
ga.domain.delete	Can delete a domain (group of published documents)
ga.docteam.admin	Can modify ALL document ownership teams in order to assign an owner
getit.admin	Provides access to the OAA Admin module.
getit.personalization.admin	Can set personalization options and save personalization changes as the default layout.
getit.personalization.default	Can change the layout and add or remove fields from Get-Answers interface.
getit.personalization.limited	Can only personalize features that have been exposed by a user with greater personalization rights.
getit.portal	Can view the OAA home page and portal components.
getit.home	Grants access to the My Home Page portal component. Lets users view a defined home page.
getit.content	Grants access to the Add or Remove Content portal component, where users can add content to, or remove it from, their home pages.
getit.language	Grants access to the Change Language portal component, where users can change the preferred language.
getit.layout	Grants access to the Change Layout portal component, where users can change the layout of the My Home Page view.
getit.skins	Grants access to the Change Theme portal component, where users can change the portal's appearance.
getit.password	Grants access to the Change Password portal component, where users can change their passwords. This requires that the Administration setting is "Enable Change Password" option on the Common tab is set to "Yes."
getit.timezone	Grants access to the Change time zone portal component, where users can change the preferred time zone setting.
oaa.forbidden	Reserved capability word to prevent access to all OAA users (cannot be granted to any user).

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.

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 or change the HIPPA security settings in the Rome database.

When a user account is created, the back-ends automatically populate the fields required by the account and password management. For example, the Rome back-end automatically calculates the Password Expiration Date.

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.

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 246.

- Use a custom configuration to authenticate users against user-defined adapters such as LDAP or JDBC compliant databases. See Custom JAAS configuration on page 247.

- 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 255.

- Use Integrated Windows authentication to authenticate users and pass the information to the Web application. See Integrated Windows Authentication on page 256.

- Use an alternate login page and authenticate users against any of the other login options. See Creating an alternate login page on page 278.

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:

Default Setting
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
`<jaas_config>` `</jaas_config>`	Define a custom JAAS configuration. All JAAS configuration settings must be between these two tags.
`<jaasConfiguration>` `</jaasConfiguration>`	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 `CustomConfig`, then you must use the tags `<CustomConfig>` and `</CustomConfig>` to define the list of adapters used.
`<CustomConfig>` `</CustomConfig>` This is a user definable tag.	Define the list of *all* 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 adapter1 and adapter2, then you must use the tags `<Adapter1>`, `</Adapter1>`, `<Adapter2>`, and `</Adapter2>` to define your adapters.
`<adapter1>` `</adapter1>` `<adapter2>` `</adapter2>` These are user definable tags.	Define the JAAS LoginModule settings for each adapter. Each adapter *must* have both `<loginModule>` and `<controlFlag>` tags defined for it.
`<loginModule>` `</loginModule>`	Define the fully qualified class name of the JAAS LoginModule. This is *required* only when authenticating against non-OAA LoginModules (adapters). The default value is `com.peregrine.oaa.archway.security.OAALoginModule.` This is *optional* only when authenticating against Peregrine back-ends.

Use these XML tags	To do this
`<controlFlag> </controlFlag>` This tag is optional.	Define the authentication behavior of this LoginModule. The default value is `REQUIRED`. See JAAS LoginModule control flags on page 249 for a description of available options.
`<options> </options>`	Define the list of authentication options. Use semicolons between entries to specify multiple options. This is an *optional* setting for each JAAS LoginModule you use. See JAAS configuration options on page 250 for a description of available options.

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.
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.
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. This is the default behavior.

Note: The 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.

Option	Use	Description
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
user.provider.url	required	Use this option to provide the URL to the starting point in your directory service where you want to search for users. For example, `ldap://server/dc=peregrine,dc=com` **Note:** This option corresponds to the Java constant `Context.PROVIDER_URL`.
security.principal	optional	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, `uid=user,dc=peregrine,dc=com` **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. **Note:** This option corresponds to the Java constant `Context.SECURITY_PRINCIPAL`.

Option	Use	Description
security.credentials	optional	Use this option to define the password for the `security.principal` user. This option should only be used in conjunction with the `security.principal` option. Note: If you are using a simple security authentication protocol, then this password may be passed as plain text. **Tip:** To safeguard this password, either enable SSL (set the `security.protocol=ssl` option) or use an `security.authentication` that protects passwords. Note: This option corresponds to the Java constant `Context.SECURITY_CREDENTIALS`.
security.protocol	optional	Use this option to enable or disable an SSL connection between the JndiLoginModule and your directory server. This option has two possible values: `simple` (Default setting) `ssl` **Note:** This option corresponds to the Java constant `Context.SECURITY_PROTOCOL`
security.authentication	optional	Use this option to enable or disable anonymous binding to your directory service. Typically, this option has one of two values: **none** (Default setting) **simple** **Note:** If you do not specify a value for `security.principal` then `security.authentication` defaults to a value of none. Likewise, if you set `security.authentication` to `simple` but `security.credentials` is omitted or has zero length, then `security.authentication` resets to none. **Note:** This option corresponds to the Java constant `Context.SECURITY_AUTHENTICATION`.
user.search.scope	optional	Use this option to specify the number of levels to descend when searching for the user being authenticated by `user.provider.url`. This value must be an integer. The default value is 1. **Note:** This option corresponds to the Java constant `SearchControls.ONELEVEL_SCOPE`.

Option	Use	Description
group.provider.url	optional	Use this option to provide the URL to the starting point in your directory service where you want to search for groups. For example, `ldap://server/dc=peregrine,dc=com` **Note:** This option corresponds to the Java constant `Context.PROVIDER_URL`.
group.search.scope	optional	Use this option to specify the number of levels to descend when searching for a group. This option should only be used with `group.provider.url`. This value must be an integer. The default value is 1. **Note:** This option corresponds to the Java constant `SearchControls.ONELEVEL_SCOPE`.

group.search.objectClass	optional	Use this option to specify the name of the LDAP group objectClass. Valid values are:
		
		`groupOfNames` (Default value)
		
		`groupOfUniqueNames`
		
		`groupOfUrls`
		
		Note: Either `groupOfNames` or `groupOfUniqueNames` can be used to define static groups in LDAP, but they may not be used together.
		
		If you choose the `groupOfUrls` option, then you are configuring dynamic groups. No additional configuration settings are required to recognize dynamic groups.

storeIdentity=true	optional	Use this option to store a reference to the User being authenticated.
clearIdentity=true	optional	Use this option to clear a reference to the User being authenticated.

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.

```
<settings>
   <jaas_config>
      <jaasConfiguration>myConfig</jaasConfiguration>
      <myConfig>ldap;ac;sc;rome</myConfig>
      <ldap>
        <loginModule>com.peregrine.oaa.security.JndiLoginModule</loginModule>
          <controlFlag>requisite</controlFlag>
           <options>
              setPreAuthenticated=true;
              user.provider.url=ldap://myldapserver:389/
                  ou=people,dc=mycompany,dc=com
          </options>
      </ldap>
   </jaas_config>
</settings>


Example with additional user capabilities stored in LDAP, see group.provider.url
option:

<settings>
   <jaas_config>
      <jaasConfiguration>myConfig</jaasConfiguration>
      <myConfig>ldap;ac;sc;rome</myConfig>
      <ldap>
          <loginModule>com.peregrine.oaa.security.JndiLoginModule</loginModule>
          <controlFlag>requisite</controlFlag>
           <options>
              setPreAuthenticated=true;
              user.provider.url=ldap://myldapserver:389/
                  ou=people,dc=mycompany,dc=com
              group.provider.url=ldap://myldapserver:389/
                  ou=groups,dc=mycompany,dc=com
          </options>
      </ldap>
   </jaas_config>
</settings>

Notes:
1) Character comparisons are case-sensitive. Be sure to match cases for all XML
tags and values.

2) Strip out all extraneous white space from with the values of elements. For
example, do not specify:
          <loginModule>
              com.peregrine.oaa.security.JndiLoginModule
          </loginModule>
Rather, use:
          <loginModule>com.peregrine.oaa.security.JndiLoginModule</loginModule>

White spaces are allowed only between semi-colon separated options within the
<options></options> tags.

Tip: To ensure your local.xml file contains valid XML formatting, open it using
InternetExplorer or some other XML viewing tool.
```

Standard Sun Microsystems JAAS configuration

The standard JAAS configuration option authenticates users against the Sun Microsytems 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 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 circumstance is an exception to the normal Integrated Windows Authentication login process:

- The Windows user name is not already registered in the back-end system. When this occurs, the Web application does not proceed with automatic login. This only occurs for users when the **Require Integrated Windows Authentication** option on the Admin page is set to No. The user sees another login screen and is asked for password verification. 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 an eight-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 258.

Step 2 Install and configure Get-Answers with Apache and Tomcat. See Preparing to configure Integrated Windows Authentication on page 258.

Step 3 Set Web server properties for the `login.asp` file. See Setting Web server properties for the login.asp file on page 258.

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 261.

Step 5 Set Web server properties for the `loginverify.asp` file. See Setting Web server properties for the loginverify.asp file on page 263.

Step 6 Set the **Require Integrated Windows 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 264.

Step 7 Set the settings on the Common tab from the Get-Answers administration page. See Updating the Common tab URL settings on page 260.

Step 8 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 265.

The following procedures illustrate how to setup Integrated Windows Authentication using Windows 2000 as an example. 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 Get-Answers, AssetCenter, or ServiceCenter administrator to verify that users have Operator records. Create an Operator record as needed.

Preparing to configure Integrated Windows Authentication

This section describes how to configure Integrated Windows Authentication if you use Tomcat as your application server, Apache as your Web server, and IIS for authentication.

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">
```

Note: If you are not using the default port (80), you must specify the port number on the URL.

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**.
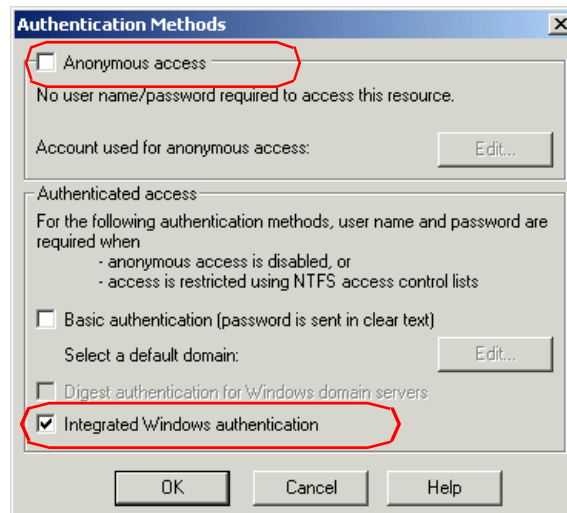
Clear the **Anonymous access** check box.

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
```
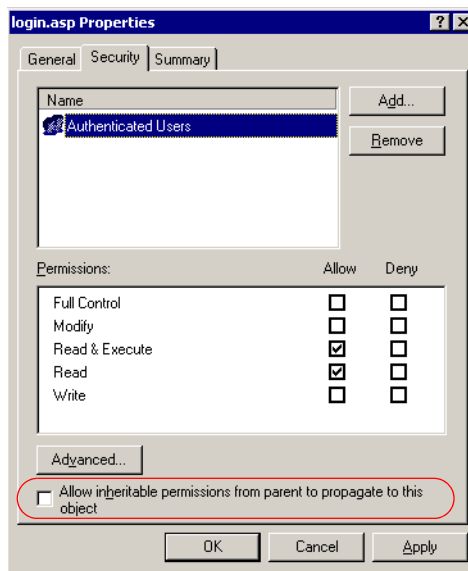

Make sure that only the Authenticated Users group is in this list.

Verify that the **Allow inheritable permissions from parent to propagate to this object** option is not checked.

    c Clear the check box beside the **Allow inheritable permissions from parent to propagate to this object** option, then click **OK**.

## Updating the Common tab URL settings

You need to set the Server URL and Login Verify URL parameters on the Common tab of the Admin Settings page.

To set the URL settings:

1 Log on the Peregrine Portal as a system administrator.

2 Click the **Administration** tab.

3 Click the **Settings** link.

4 On the Common tab, set the following parameters:

■ Server URL - This must be the fully qualified Apache Web server / IIS server URL to the OAA virtual directory. The URL must include the port number if it is not 80.

■ Login Verify URL - This must be the fully qualified IIS server URL to the OAA virtual directory. The URL must include the port number if it is not 80.

Example: `http://DP8417:87/oaa_authentication`
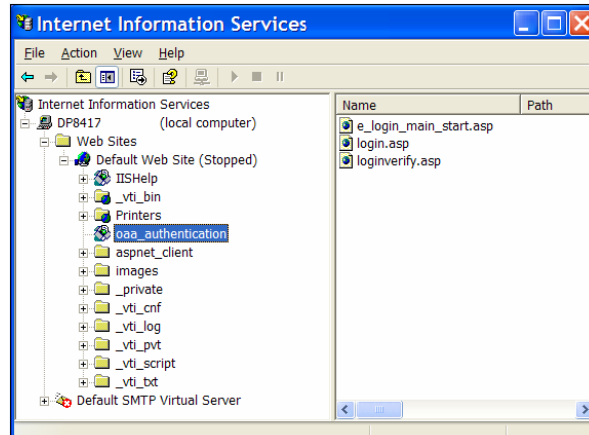
Setting Web server properties for the e_login_main_start.asp file

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>
/oaa/e_login_main_start.do" method="post">
```

Note: If you are not using the default port (80), you must specify the port
      number on the URL.

2   Open the IIS Management Console (click **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**.
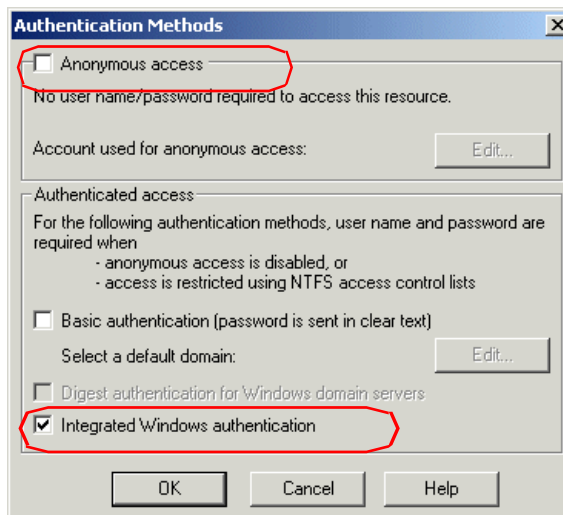
Clear the
Anonymous access
check box.

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
    ```
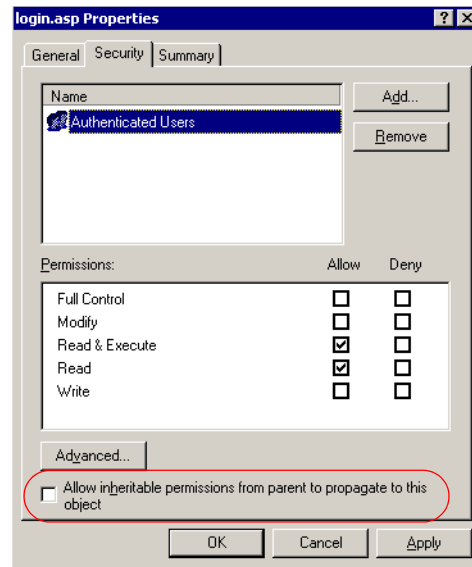

Make sure that only the
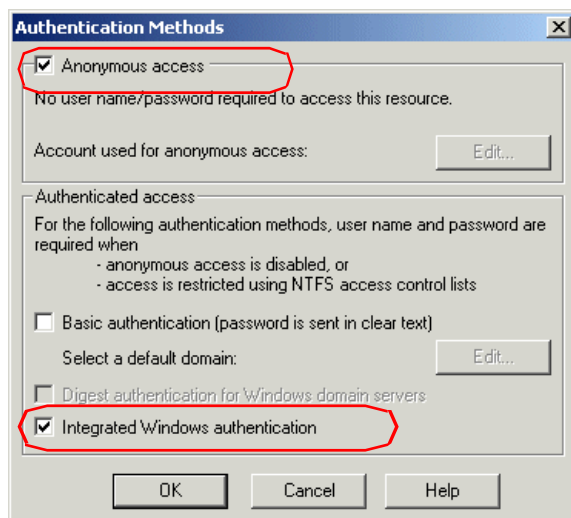Authenticated Users
group is in this list.

Verify that the **Allow
inheritable permissions from
parent to propagate to this
object** option is not checked.

    c   Clear the check box beside the **Allow inheritable permissions from
        parent to propagate to this object** option, then click **OK**.

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 Integrated Windows 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 Integrated Windows 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**.
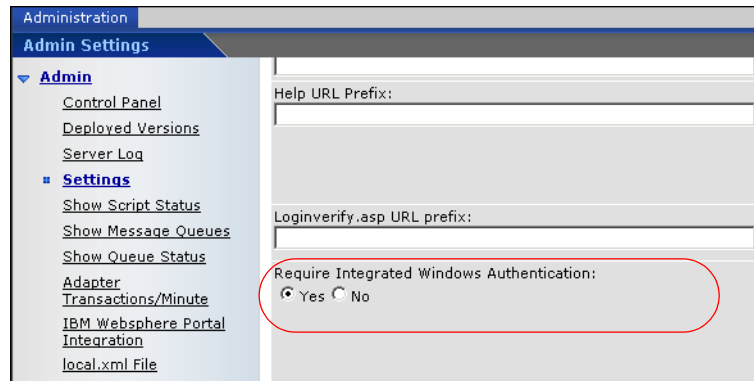
5   From the **Common** tab, set the **Require Integrated Windows
     Authentication** parameter to Yes.

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 Peregrine Portal**.

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 Setting the Admin parameters on
     page 264), 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 Peregrine Portal**.

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>:<port>/<oaa>/login.asp* in the browser address field (where `<webserver>` is the name of your Web server, and `:<port>` is only required if it is other than port 80, 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.

Once you have verified this setting, all the users authenticated by Integrated Windows Authentication should now access Get-Answers with the `login.asp` URL.

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 256.

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 a 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:

```
<%@ 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>
```

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`.

Authentication models

The following sections discuss:

- ServiceCenter authentication components
- OAA contact and operator associations
- Regular operator authentication
- Contact-based authentication

ServiceCenter authentication components

There are two components of the ServiceCenter authentication model: the `Operator` file and the `Contacts` file.

The `Operator` file contains the following keys.

Key	Description
name field	This is the primary key (unique and indexed).
full.name field	This is a foreign key to the contact table. It represents the contact associated with the operator. It is indexed, it can be empty, and several operators can have the same value for this field. The value of the full.name field, when not empty, represents the value of the contact.name field in one of the records in the contacts file.

The `Contacts` file contains the following keys.

Key	Description
contact.name field	This is the primary key; it is unique and indexed.
user.id field	This is indexed and is a "no duplicate" field; it can be null, but must be unique if not null. When contact-based authentication is enabled, the user.id field is the key used to look up contacts.

OAA contact and operator associations

OAA approaches contact and operator handling by allowing ServiceCenter administrators to customize their `Contacts` and `Operator` files, and to use `Contacts` and `Operator` associations that differ from OAA defaults.

The OAA schemas allow flexibility in defining associations between records in the `Contacts` and `Operator` files. These OAA schemas provide a logical view that is "wrapped around" their physical implementations. OAA provides attribute names that correspond to each type of lookup operation. Therefore, for an administrator, customizing the lookup is as simple as creating a schema extension on the `Profile` or the `Contact` schema.

For more information about schemas, see the Schemas chapter in this guide.

Important: If you create schema extensions for either the Contact schema or the Profile schema, ensure that their corresponding fields in the Contacts file and the Operator file are both unique (no duplicates) and indexed to maintain adequate performance during table look ups.

Regular operator authentication

Name and password pairs are validated against the existing operator in the operator table. In addition, the presence of the operator's contact is queried based on the fields mentioned below.

Algorithm for looking up contacts

The Contact schema has the following attributes.

Logical name	Mapping in profile schema	Mapping in contact schema
OperatorContactKey1	full.name	contact.name
OperatorContactKey2	name	user.id

Using these attributes, the lookup algorithm is the following:

1   Read the values for OperatorContactKey1 and OperatorContactKey2 in the `Profile` schema whose UserName equals the UserName (login name) of the logged in operator.

2   Search the `Contact` schema for a record whose Id is the value of OperatorContactKey1.

3   If exactly one record is found, return this contact's Id.

4   If no record, or more than one record, is found, search the `Contact` schema for a record whose Id equals the value of OperatorContactKey2.

5   If exactly one record is found, return this contact's Id.

6   If no record, or more than one record, is found, return null and attempt to create the contact, if required. (See the following Contact creation section.)

Contact creation

If an operator's contact record is not found during contact lookup, OAA does not create a contact automatically. A setting in the Get-Answers Admin module under the ServiceCenter tab controls this behavior: `Create a Contact record for the Operator during login`. The default setting is No, which does not create a contact record for the operator during login. When set to Yes, a contact record is created for the operating during login if the contact record does not already exist.

All the information from the Profile record for the logged in operator is used to create a Contact record. Therefore, all the Profile values that have a corresponding attribute in the `Contact` schema are saved in the database. In addition, the Contact record's ProfileId (see Logical mapping) is assigned the value of the Profile record's Id to establish a mapping from the Contact back to the Profile. The following tables describe both the logical and physical mappings of particular fields of interest during contact creation.

Logical mapping

Logical name in Profile schema	Logical name in Contact schema
Id	ProfileId
UserName	UserName
FullName	Id

Physical mapping

Physical name in Profile schema	Physical name in Contact schema
name	operator.id
name	user.id
full.name	contact.name

Contact-based authentication

This section describes an alternate authentication scheme that automatically verifies Windows users as ServiceCenter contacts.

When logging in through `loginContactBased.asp` or one of its copies, the user will be logged in if a contact exists for this user in ServiceCenter. The user gets the ServiceCenter profile and capability words from a ServiceCenter operator. The same operator performs all ServiceCenter operations on behalf of the user.

The setting of the `With CBA, give Operators their Operator capabilities` attribute under the ServiceCenter tab controls how the operator is determined.

Setting option	What the setting determines
Yes	The operator defined on the contact record in ServiceCenter is used. If no operator is defined in the contact record, the default operator defined in `local.xml` is used.
No (default setting)	The default operator set in the `local.xml` file (see Editing the local.xml file on page 277) is used.

Note: The following authentication scheme requires that both the user who is logged into the machine running the client browser *and* the IIS server reside either in the same domain, or in different domains that have a trusted relationship.

Perform the following steps to set up your server:

Step 1   Create a contact record in ServiceCenter for each Windows user who you want to be able to log in. See Creating a contact record on page 273.

Step 2   Choose or create one Operator record in ServiceCenter that will be the default operator. See Creating a default Operator record in ServiceCenter on page 273.

Step 3   Configure each login ASP file for Integrated Windows Authentication. See Changing the authentication method in IIS on page 274.

Step 4   Verify the Integrated Windows Authentication setting on the Get-Answers Admin module Settings page. See Verifying the Get-Answers Admin setting on page 276.

Step 5   Edit `local.xml` in `<application server>\oaa\WEB-INF` to define the passwords for the default operator. The step is optional; do this only if you want to set up a default operator. See Editing the local.xml file on page 277.

Step 6   Restart the application server.

Creating a contact record

Create one contact record for each Windows user who you want to log in. The Employee ID (userid) field of the contact record must match the Windows user name exactly, including upper- and lower-case.

For more information about creating contact records, see the ServiceCenter Application Administration online help.

Creating a default Operator record in ServiceCenter

Refer to your ServiceCenter documentation for information on adding Operator records.

Assign the Get-Answers capability words that you want your users to have by default.

Changing the authentication method in IIS

You must configure `loginContactBased.asp` or its copies. This requires changing the authentication method in IIS.

To change the authentication method in IIS:

1   Open the IIS Management Console (click **Start** > **Programs** > **Administrative Tools** > **Internet Information Services**).

2   Navigate to the `oaa` virtual directory.

3   Navigate to `loginContactBased.asp`.

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**.
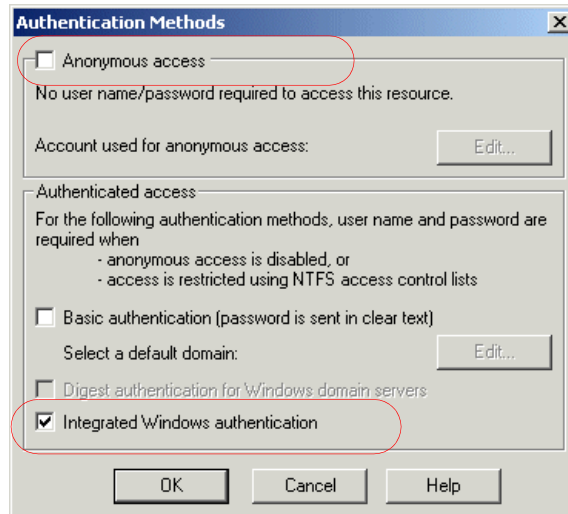
Clear the Anonymous
access check box.

Select the Integrated
Windows authentication
check box.

7   Click **OK** on all windows displayed until you return to the Microsoft
    Management Console.

Verifying the Get-Answers Admin setting

From the Get-Answers Admin module, you must verify that the **Require Integrated Windows Authentication** option is set to No. If set to Yes, users accessing `login.jsp` directly might be logged in with no access to ServiceCenter or the login might fail.

1   Log in to the Get-Answers Admin module, click Settings, then click the Common tab.

2   Scroll to the Encoding, Locales, and Sessions section.

3   Make sure that the option **Require Integrated Windows Authentication** is set to **No**.

Require Integrated Windows Authentication:
○ Yes ● No

Set to true to allow only users who are preauthenticated by Windows to log in. You must configure Integrated Windows Authentication (IWA) as described in the setup guide before enabling this option. Set this together with the Logout URL option.

Editing the local.xml file

In the `local.xml` file, you must specify the operator name and password for the scdefault alias. This file is located at:
`<application server>\oaa\WEB-INF\local.xml`.

To edit the local.xml file:

1   Using a text editor, open `local.xml`.

2   Add two XML entries.

The tags have the format:

`<scdefault>operator</scdefault>`

and

`<scdefaultPassword>password</scdefaultPassword>`

For example, for operator `Tossi` and `scdefault`, add the following inside the `<settings> ... </settings>` tags.

```
<scdefault>Tossi</scdefault>
<scdefaultPassword>Tossi_password</scdefaultPassword>
```

where `Tossi_password` is the ServiceCenter password assigned to operator `Tossi`.

Important: The password must match the Operator password in ServiceCenter.

Restarting the application server

You must restart the application server for your changes to take effect.

Tailoring contact-based authentication

OAA uses the ServiceCenter `user.id` field in the Contacts file to look up a contact for contact-based authentication. However, some administrators use this field to hold employee IDs (such as numeric employee IDs, badge numbers, and Social Security numbers) rather than network names (network names are applicable when Integrated Windows Authentication is enabled). UserName is the logical name in the Contact schema for the `user.id` field. Through a schema

extension, administrators can customize this to point to a different field or a newly defined field.

Similarly, the Profile schema defines UserName to maintain data integrity and facilitate customization. Creating a schema extension for this usually is not necessary. For more information, see the Schemas chapter of this guide.

Schema type	Logical name	Physical name
Contact	UserName	user.id
Profile	UserName	name

Important: If you create a schema extension for UserName for either the Contact schema or the Profile schema, ensure that their corresponding fields in the Contacts file and Operator file are both unique and indexed to maintain adequate performance during table look ups.

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 `local.xml` file to specify the HTTP authentication method you want to use. See Specifying an alternate authentication method on page 280.

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 fail to be successfully authenticated should see the page that is specified in the `_failURL` value. This can simply point to your login page so that the user can re-attempt login.
- 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.
- 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.
- The following login parameters are available:

Login parameters	Description
loginuser	This is a required login parameter specifying the user name. You must specify a form input for this parameter.
loginpass	This is a required login parameter specifying the login password. You must specify a form input for this parameter.
_locale	This is an optional login parameter specifying the user's locale and regional display settings.
_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 `local.xml` file.

To specify an alternate HTTP authentication method:

1   Stop your application server.

2   Using a text editor, open the `local.xml` file located at:

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

3   Add the following entry to local.xml below the <settings> element (if the entry does not already exist):

 `<HTTPAuthClass>HttpAlternateAuthenticationManager</HTTPAuthClass>`

4   Save the file.

5   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.

6   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, changing your database password in the Get-Answers Search Engine configuration files, customize the rich 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

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 284.)
- How words you add or remove from the Stop Words list affect searching in Get-Answers. (See New and deleted Stop words on page 285.)
- How to add or remove Stop words from the Stop Words list. (See Modifying the Stop Words list on page 287.)

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)
- 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   From the Start menu, choose **Programs**> **Get-Answers Search Engine**> **System Utilities Menu**.

2   Choose option 6 - Indexing and index utilities.

3   Choose option 11 - Delete and create empty indexes for a library.

4   At the "Indexes should be deleted for which library? Enter Library Name []>"
     command prompt, type KMLib.

5   At the "Are you sure? (1 = YES, 2 = NO)" command prompt, type 1.

     These messages appear:

     ```
     Opening Library: KMLib
     Thank you!
     ```

6   Press any key to continue.

7   Choose option 1 - Return to previous menu.

8   Choose option 1 - Exit this program.

9   From the Start menu, choose **Programs**> **Get-Answers Search Engine**>
     Start Search Engine Server.

     These messages appear:

     ```
     Starting up the Search Engine Server
     Press any key to continue . . .
     ```

10   From the Start menu, choose **Programs** > **Get-Answers Search Engine** >
     Reindex all Documents.

11   At the "Enter the name of the library to be indexed. Enter Library Name []>"
     command prompt, type KMLib.

12   At the "Are you sure you wish to index the entire RDBMS now? (warning: this
     will delete any existing indexes in KMLib). (1 = YES, 2 = NO)" command
     prompt, type 1.

     This message appears:

     ```
     All records have been submitted to the document handler.
     ```

13   Press any key to continue.

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.
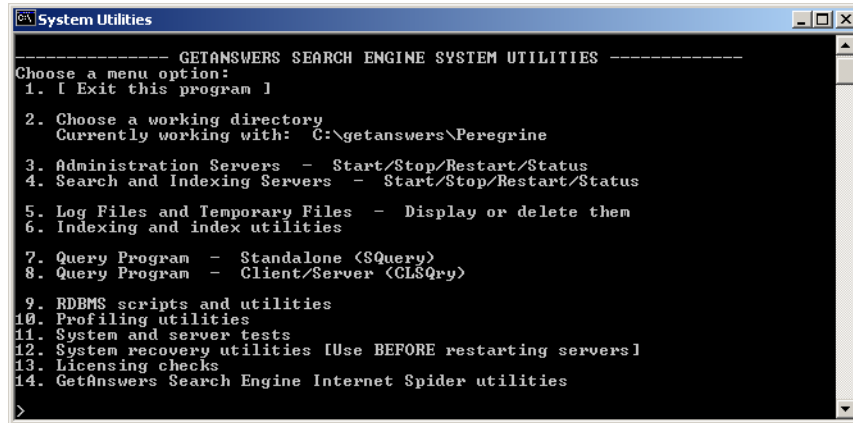
Expansion Word List and Level in a Concept Search

Checking a word's expansion may be useful in understanding why a particular highlighted word is returned in a Get-Answers search.

To check the word expansion for a particular term:

1   At the Search Engine Server, click **Start Programs** > **Get Answers Search Engine** > **System Utilities**.

2   Type **7** for Query Program - Standalone (SQuery) and then press the **Enter** key.

3   Type **1** to select library KMLib and the press the **Enter** key.

4   Type **C** and then press the **Enter** key.

5   Type **M** (for Menu) and then press the **Enter** key.

A new command window opens for the OTHER OPTIONS MENU.

```
CONCEPT > m


OTHER OPTIONS MENU
  1.   Return to the query program
  2.   Save user variables in file: squery.ini
  3.   Set the level to which words are expanded (currently 4)
  4.   Set query type (currently CONCEPT)
  5.   Change screen parameters (currently 80 x 25)
  6.   Set document list display options
  7.   Go to dictionary menu
  8.   Set Query By Example number of words (currently 50)
  9.   Set expansion options, including maximum number of words for
       wildcards (50), fuzzy spelling (15), and semantic expansions (20)
 10.   Set the default date format (currently Month/Day/Year)
 11.   Set sorting and retrieval options
 12.   Toggle phrase handling method ( currently Exact )
 13.   Open Private Query Dictionary
 14.   Set meaning of single-quoted words.
 15.   Set arbitrary properties.
 16.   Set view parser state.
Enter an option number and then press RETURN ( 1 ):
```

The options available are:

1. Return to the query program

2. Save user variables in file: squery.ini

3. Set the level to which words are expanded (currently 4)

4. Set query type (currently CONCEPT)

5. Change screen parameters (currently 80 x 25)

6. Set document list display options

7. Go to dictionary menu

8. Set Query By Example number of words (currently 50)

9. Set expansion options, including maximum number of words for wildcards (50), fuzzy spelling (15), and semantic expansions (20)

10. Set the default date format (currently Month/Day/Year)

11. Set sorting and retrieval options

12. Toggle phrase handling method (currently Exact)

13. Open Private Query Dictionary

14. Set meaning of single-quoted words.

15. Set arbitrary properties.

16. Set view parser state.

6   Type **3** for Set the level to which words are expanded (currently 4) and then press **Enter**.

The command window displays the levels available.
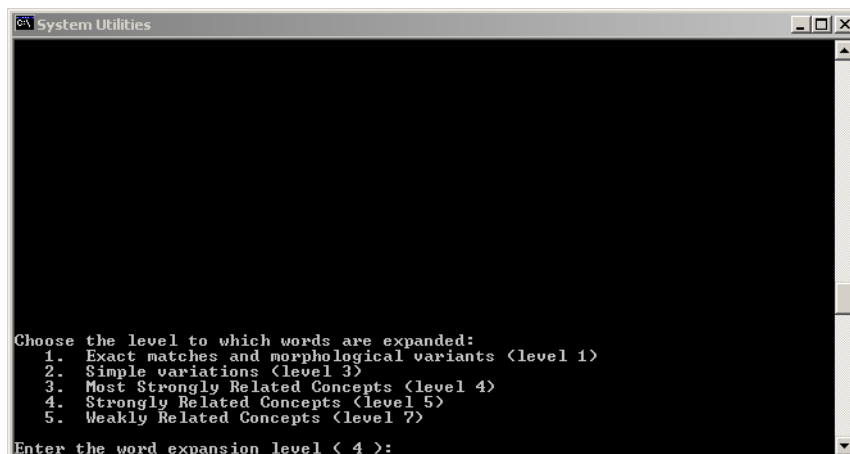
The levels to which words are expanded are:

1. Exact matches and morphological variants (level 1)

2. Simple variations (level 3)

3. Most Strongly Related Concepts (level 4)

4. Strongly Related Concepts (level 5)

5. Weakly Related Concepts (level 7)

7   Select a level and press **Enter**.

A command window displays the OTHER OPTIONS MENU.

8   Type **7** for Go to dictionary menu and press **Enter**.
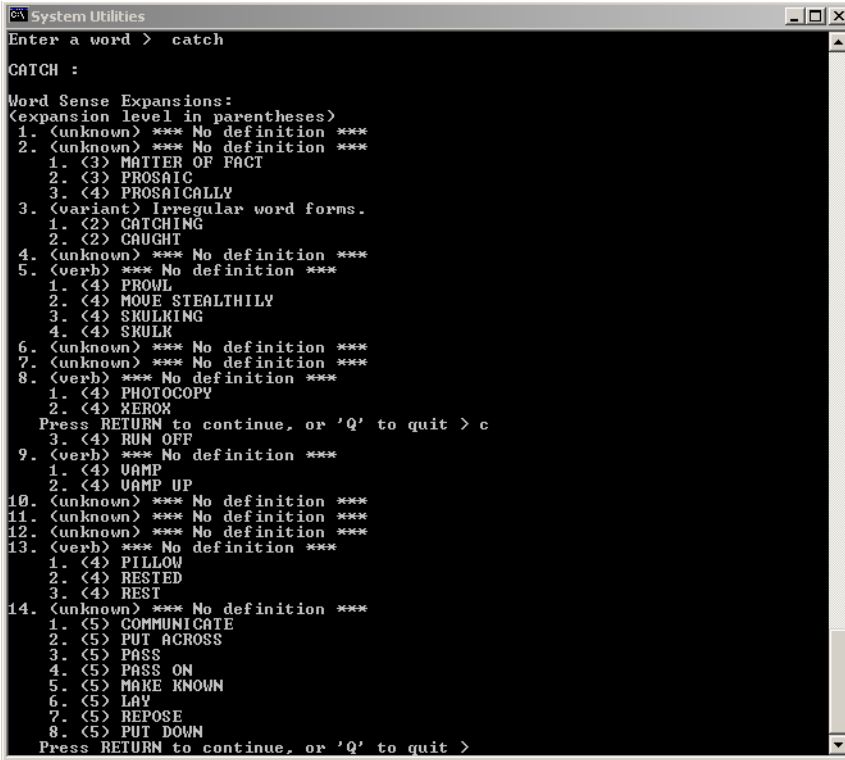
A command window displays the DICTIONARY FUNCTION MENU.
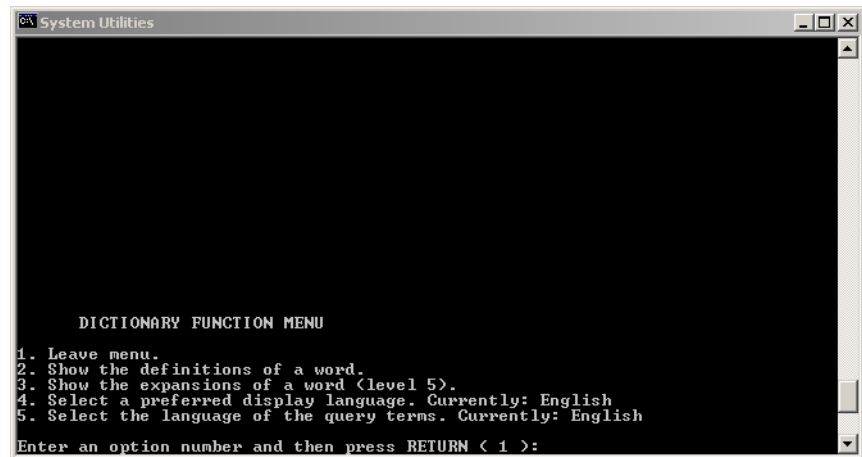
This menu contains the following choices:

1. Leave menu.

2. Show the definitions of a word.

3. Show the expansions of a word (level x).

4. Select a preferred display language. Currently: English

5. Select the language of the query terms. Currently: English

9   Type **3** for Show the expansions of a word for the level that you chose and press **Enter**.

10   Type the word. For example if you type the word, catch you are presented with many Word Sense Expansions, some of which are synonyms or

antonyms for the word you entered. The number in parentheses that precedes the word is the expansion level.


```
System Utilities                                               _ □ ×
Enter a word >  catch                                             ▲

CATCH :

Word Sense Expansions:
(expansion level in parentheses)
 1. (unknown) *** No definition ***
 2. (unknown) *** No definition ***
    1. (3) MATTER OF FACT
    2. (3) PROSAIC
    3. (4) PROSAICALLY
 3. (variant) Irregular word forms.
    1. (2) CATCHING
    2. (2) CAUGHT
 4. (unknown) *** No definition ***
 5. (verb) *** No definition ***
    1. (4) PROWL
    2. (4) MOVE STEALTHILY
    3. (4) SKULKING
    4. (4) SKULK
 6. (unknown) *** No definition ***
 7. (unknown) *** No definition ***
 8. (verb) *** No definition ***
    1. (4) PHOTOCOPY
    2. (4) XEROX
   Press RETURN to continue, or 'Q' to quit > c
    3. (4) RUN OFF
 9. (verb) *** No definition ***
    1. (4) VAMP
    2. (4) VAMP UP
10. (unknown) *** No definition ***
11. (unknown) *** No definition ***
12. (unknown) *** No definition ***
13. (verb) *** No definition ***
    1. (4) PILLOW
    2. (4) RESTED
    3. (4) REST
14. (unknown) *** No definition ***
    1. (5) COMMUNICATE
    2. (5) PUT ACROSS
    3. (5) PASS
    4. (5) PASS ON
    5. (5) MAKE KNOWN
    6. (5) LAY
    7. (5) REPOSE
    8. (5) PUT DOWN
   Press RETURN to continue, or 'Q' to quit >            ▼
```

For Example, these are the expansions for Strongly Related Concepts (Choice 4, level 5) for the word catch:

> 1. (4) PILLOW

> 2. (4) RESTED as in to sleep or catch a nap / catch 30 winks / catch some
>   zzz

> 3. (4) REST

11 To exit:

- Type Q and press Return.
- Type 1and press Return.
- Type 1 and press Return.

- Then Q and Return to exit the program.
- Type Y for yes.
- Type 1 to exit.

Checking a word's expansion may be useful in understanding why a particular highlighted word is returned in a Get-Answers search. For more information on Advanced Search, see the *Get-Answers User's Guide*, Chapter 1, Finding Information in Get-Answers and Appendix A, Search Queries.

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.

File	Description
`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 .

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.

   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
```

4   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.

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:

Line	Description
First Line	A period (.)
Second LIne	Exclamation point symbol (!) followed by a comment.
Third Line	The "at" symbol (@), followed by a single upper-case character denoting the part of speech (e.g., N).
Fourth 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(.)

c   End the file with a blank line after the last period (.).

For example:

```
.
! Family dogs
@N
28 RETRIEVER
28 MYDOGSPOT
28 SPOT
28 GOLDEN
28 DOG
28 GOLDEN RETRIEVER
28 MY DOG SPOT
.
!Prized cats
@N
28 PERSIAN
28 MYARISTOCAT
28 ARISTOCAT
28 EXPENSIVE
28 CAT
28 EXPENSIVE CAT
28 MY ARISTOCAT
.
```

2   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
```

6 Also, re-index the user dictionary, "userdict" with the following command:

```
C:\getanswers\bin\dict_xrf.exe c:\getanswers\resource\rw_english\userdict
```

7 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.

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-AnswersSearchEngine4.2** > **Stop Search Engine Server**.

2 Restart the Get-Answers Search Engine. To do this by default, select **Start > Programs** > **Get-AnswersSearchEngine4.2** > **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   Within five minutes, your new documents are indexed.

3   Search for a related term from your group, for example, SPOT.

You should get a hit on your document.

Changing your database password in the Get-Answers Search Engine configuration files

This section describes the steps an administrator needs to complete to change the database password in the Get-Answers Search Engine configuration files.

To change your database password in the Get-Answers Search Engine configuration files:

1   In a command window n your search engine server, navigate to the `<Search_Engine_Directory>\bin` folder.

On a default installation on Windows, this is located in:

```
C:\getanswers\bin\
```

2   Using the following command, substitute your current password for yourPassword type:

```
rw_encrypt.exe -pw yourPassword
```

The `rw_encrypt` application returns an encrypted value such as:

```
lvw5%2FUgz9oo
```

3   Save the encrypted value returned by `rwencrypt`. You will use this value in the yourEncryptedPassword substitutions below.

For example:

`rw_encrypt.exe -pw db2admin`

returns

`lvw5%2FUgz9oo`

`db2admin` is yourPassword and `lvw5%2FUgz9oo` is yourEncryptedPassword.

4   Repeat step 3 with `yourNewPassword`. The encrypted value returned will be `yourNewEncryptedPassword` for the substitutions below in the search engine configuration files.

For example:

`rw_encrypt.exe -pw W2chik3n`

returns

`BUcn2Z2pGE0`

`W2chik3n` is yourNewPassword and `BUcn2Z2pGE0` is yourNewEncryptedPassword.

To modify the search engine configuration files to change your password:

1   Open the `rware.cfg` file in `<Search_Engine_Directory>\KMLib\config\` with a text editor.

a   Change every occurrence of yourPassword to yourNewPassword.

For example: change every occurrence of `db2admin` to `W2chik3n`.

b   Change every occurrence of `yourEncryptedPassword` to `yourNewEncryptedPassword`

For example: change every occurrence of `1vw5%2FUgz9oo` to `BUcn2Z2pGE0`.

   c Save the `rware.cfg` file.

2   Open the file, `exec.cfg`, located in `<Search_Engine_Directory>\KMLib\config\` with a text editor.

   a Change every occurrence of `yourPassword` to `yourNewPassword` using the same values for yourPassword and `yourNewPasword` as in did in the `rware.cfg` file.

   b Change every occurrence of `yourEncryptedPassword` to `yourNewEncryptedPassword`, if any.

   c Save the file, `exec.cfg`.

3   Open the file, `admin.dat`, located in `<Search_Engine_Directory>\KMLib\config\` with a text editor.

   a Change every occurrence of `yourPassword` to `yourNewPassword`.

   b Change every occurrence of `yourEncryptedPassword` to `yourNewEncryptedPassword`.

   c Save the `admin.dat` file.

4   Open the file, `kcs.cfg`, located in `<Search_Engine_Directory>\bin\` with a text editor.

   a Change every occurrence of yourPassword to `yourNewPassword`, if any.

   b Change every occurrence of yourEncryptedPassword to `yourNewEncryptedPassword`.

   c Save the file, `kcs.cfg`.

5   Open the file, `gaodbc.bat`, located in `<Search_Engine_Directory>\bin\` with a text editor.

   a Change every occurrence of yourPassword to yourNewPassword.

    b Change every occurrence of `yourEncryptedPassword` to `yourNewEncryptedPassword`, if any.

    c Save the file, `gaodbc.bat`.

6 Open the file, `menu.bat`, located in `<Search_Engine_Directory>\bin\` with a text editor.

    a Change every occurrence of `yourPassword` to `yourNewPassword`.

    b Change every occurrence of `yourEncryptedPassword` to `yourNewEncryptedPassword`, if any.

    c Save the file, `gaodbc.bat`.

7 Test the database connection to verify your changes.

    a On Windows, the database connection can be tested using the Get-Answers Search Engine.

    Start -> Programs -> Get-AnswersSearchEngine -> Check Database Connection

    b The following message should appear in the command (cmd) window

```
Successfully tested the connection to the Relational Database.
```

Customizing edit-on Pro

Get-Answers provides users with a rich text editor, edit-on Pro, for adding content and documents to the system. The edit-on Pro rich text editor is provided as a Java Applet. 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 Netscape Navigator 6.x, 7.x and Mozilla 1.x with Sun JRE 1.4.2_05:

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   Log on to Get-Answers as a user with Submitter permissions.

2   Contribute a document for one of the following document types:

- Problem/Solution
- How-To
- Reference
- Error Message/Cause

3   A "Warning-Security" notification dialog box in Microsoft Internet Explorer or in Netscape Navigator appears.

4   To continue loading the edit-on Pro signed applet, click "Yes". To abort loading, click "No". The "Always" 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.

Removing RealObjects from trusted publisher

To remove RealObjects from Granted Vendors in Internet Explorer or Netscape Navigator:

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.

Customizing the edit-on Pro spelling checker

You can customize the spelling checker used in the edit-on Pro authoring tool. Get-Answers determines the locale of the user and loads the `oaa/eopro/config_<locale>.xml` file to determine which spelling checker to use. For example, the `<spelling checker>` line in the `config_en.xml` file lists `default="true"` for `name="LANGUAGE-AMERICAN"`. In this example then, for English, this is the default spelling checker.

Special character translations

This section describes the special character translations for ServiceCenter and DDE integrations.

Special character translations for ServiceCenter and Get-Answers integrations

When an operator retries a solution from Get-Answers into ServiceCenter, the document data retrieved must be converted from Get-Answers format (HTML) to ServiceCenter plain text format. Get-Answers handles this translation automatically and most implementations you will not need to change or add to the delivered translation.

Get-Answers does, however, provide a mechanism for overriding and adding to the delivered translation. Administrators can create a plain text file to specify overrides and/or additions to the delivered translation. This file must adhere to the following format

`&HTML` Encoded character; "replacement character or string of characters" <cr>

Example:

```
   " "
&auml; "a"
```

`&ISO` Entity Name; "replacement character or string of characters" <cr>

Example:

```
&#149; ""
```

`<HTML  TAG>`; "replacement character or string of characters" <cr>

Example:

```
<table> "\n"
</table> "\n"
</tr> "\n"
</td> "\t"
<li> "* "
<p align="left"> ""
</p> "\n"
<p> ""
```

Note: This mechanism should be used sparingly because a large number of character translation mappings could have a negative impact of the performance of the Retrieve Solution integration function.

If you create an additional translation file, a URL to file must be accessible by the application server. This URL must be specified in the ServiceCenter Integration Character Map field on the Get-Answers tab of the Admin Settings page.

Special character translations for DDE integrations

The table, `EntityHash.txt`, which is located in:

```
C:\Program Files\Peregrine\Common\Tomcat4\webapps\oaa\dde
```

enables bi-directional translation of special characters between the actual character and the html ISO entities for the character when integrating between DDE and Get-Answers. This table is not 100% inclusive as new characters may be added with changes to the ISO standard. If you have a special character that is not listed, you may add it to the list with the following format:

```
&ISO Entity Name;  'actual character' <cr>
```

Be sure to use a carriage return at the end of the line. You may use the format "$#Hex;" for the ISO Entity Name but this method should be discouraged since not all browsers may be using the same character set and could render the wrong character during translation.

The EntityHash.txt file is loaded once when the Get-Answers DDE integration applet starts up. Any changes to EntityHash.txt may require browser restarts for all connected clients before the change take effect for them.

10 CHAPTER | Get-Answers Workflows

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. Workflows is a complex and sophisticated module of Get-Answers, please consult with Peregrine Professional Services or Support before attempting to change/customize the provided out-of-the-box workflows.

This chapter describes how to use workflow in general and includes the following topics:

- Defining workflow templates on page 311
- Using Workflow Administration on page 344
- Using the Request List on page 365

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:

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 Get-Answers to display the Navigation Menu on your Home page.
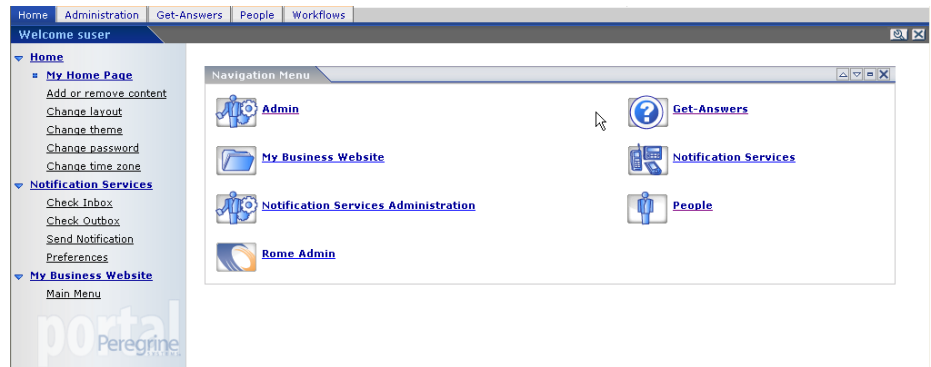
2   Click the Workflows tab or click **Workflows** from the Navigation Menu.

3   Click the **Templates Design link** to display the **List of Workflow templates** page.
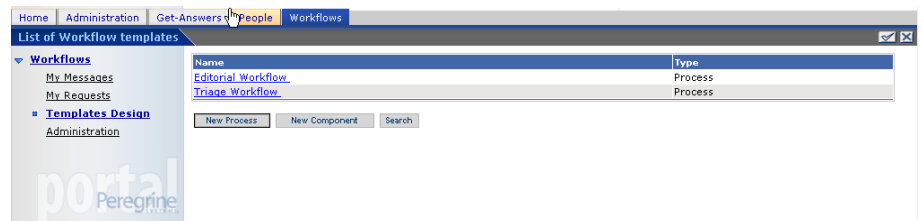
Note: When you define a new workflow templates, the template name and type (Process or Component, for each template appears in the list.

4   Click **New Process**.

The **Create a New Workflow template** page appears.
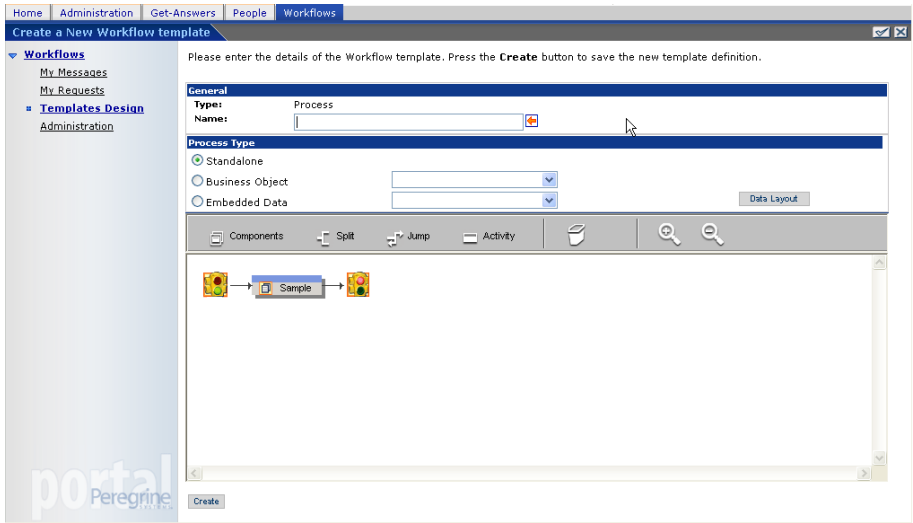
The Type of Process entry is created by the system based on your selection of the **New Process** button.

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.

Option button	Description
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 Get-Answers 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.

The window that opens depends upon which item you select.

You can change the data layout using the **Personalize this page** option at the top of the page. Refer to your Get-Answers 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 337 and Deleting an activity on page 337.

9   In the workflow designer, create and add activities to the workflow template using the toolbar icons described in the following table.

Icon	Description
Components	Select a component from the template list. See To add a component template: on page 335 for information on adding an activity from the template list.
Split	Create a new Select activity. See To create and add a Select activity: on page 329 for information on adding a Select activity.
Jump	Create a new Jump activity. See To create and add a Jump activity: on page 332 for information on adding a Jump activity.
Activity	Create a new activity. See To create and add a new activity: on page 316 for information on adding a new activity.
	Trash. See To delete an activity: on page 338 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:

1   Position the cursor over the **Activity** icon, then click and hold down the left mouse button.

2   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.

3   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).
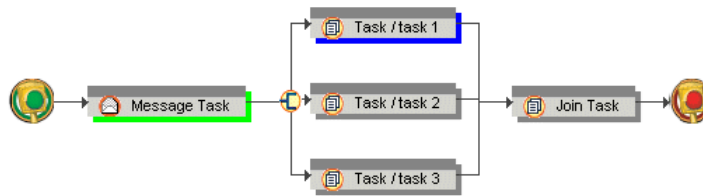
After you click the mouse button, the **Workflow** window opens. You define the details for the new activity through this window.

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:

Type value	Description
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 320.
- Message, see To complete the activity details for a Message task: on page 324.
- Script, see To complete the activity details for a Script task: on page 326.

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.

Whom to notify	Description
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 by E-mail, select the "Notify Assignee of this task" check box.

Note: The user is notified by E-mail, which is the default method indicated in the options provided in Notification Services activity under the Home tab. Get-Answers has customized the Notification Services E-mail messages so that users can review their workflow tasks and go directly to the details link in their E-mails. For more information refer to the Notification Services 4.2 Quick Start Guide. Each E-mail notification contains standard message text and a direct link to the appropriate application.

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.

Important: This step is valid only if this is not a Get-Answers activity. If this is a Get-Answers activity and you check **Auto complete upon deadline**, you will orphan the unpublished document and make it inaccessible in the Get-Answers GUI.

You can set an alarm for a time-sensitive task.

8   Select the alarm type from the **Type** drop-down list.

Values are:'

Value type	Description
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.

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.

Whom to notify	Description
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 options provided in Notification Services under the Home 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.

Note: Options a and b in this step should only be used by trained Professional Services personnel.

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.

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.
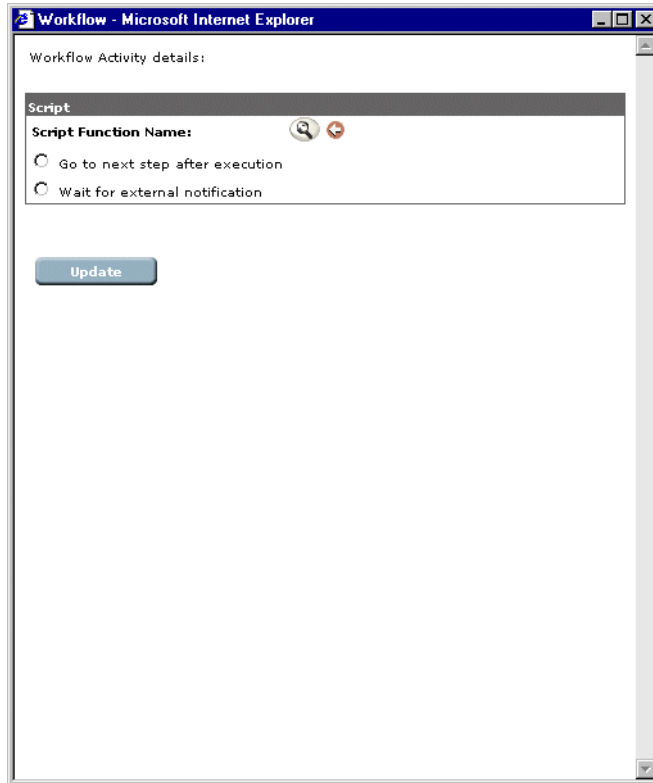
1   Click the **binoculars** next to **Script Function Name** to display the Script File Lookup window.
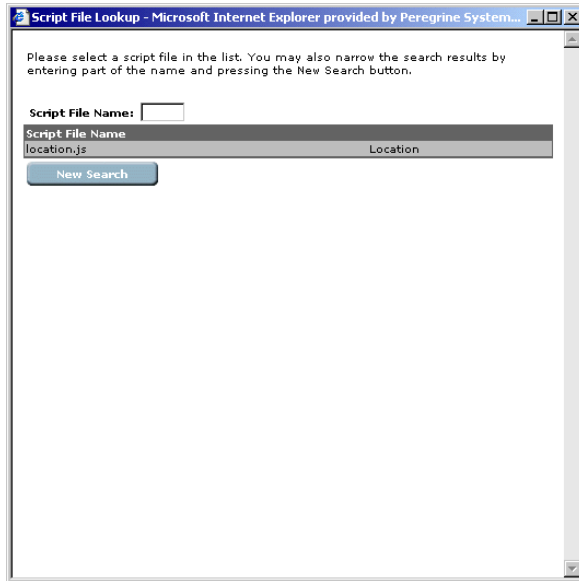
2   Using this window and following the lookup instructions, locate and select the script function.

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.

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:

Value	Description
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.
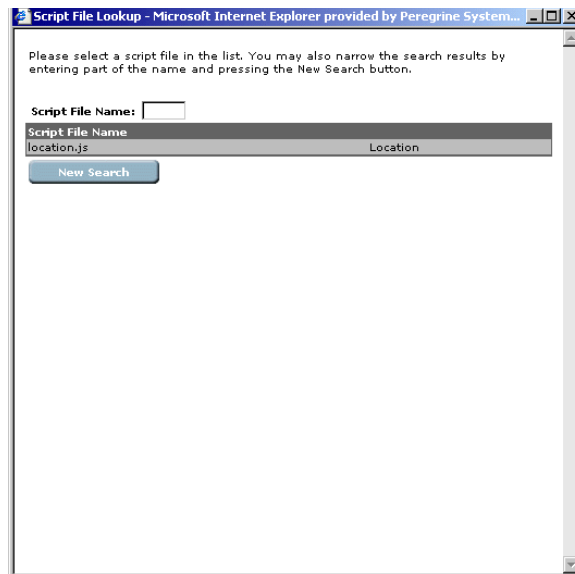
7   Using this window and following the lookup instructions, locate and select the script function.

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 337 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
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 appears.
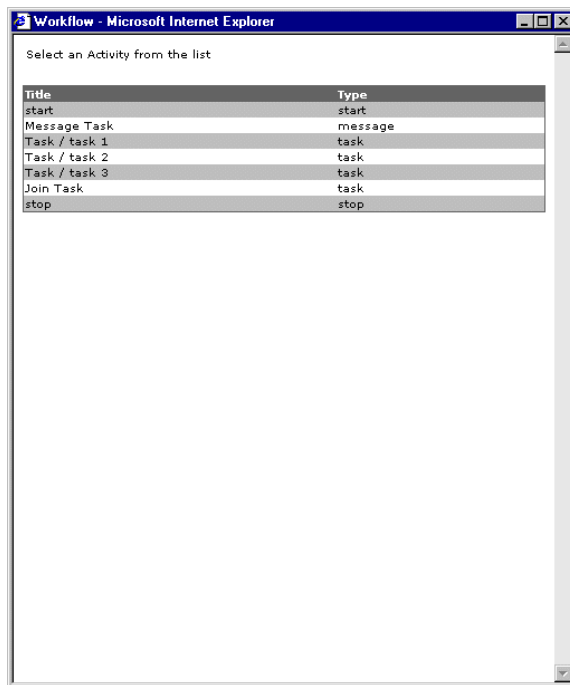
3   From the activity list, select the destination activity for the jump.

The title of the destination activity appear 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 341.

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.
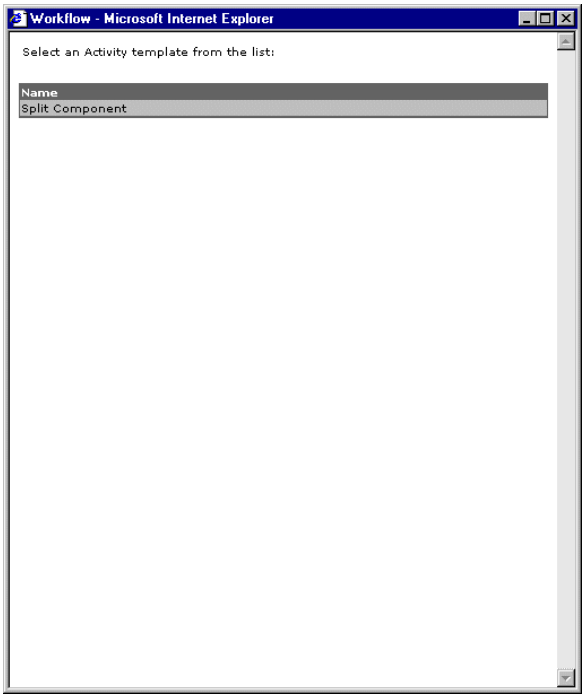
3   Click the component template you want to add to the workflow template.

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 316, Creating a Select activity on page 328, Creating a Jump activity on page 332, or Adding a Component Template on page 335 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 Get-Answers.

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 312 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 Get-Answers.

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.
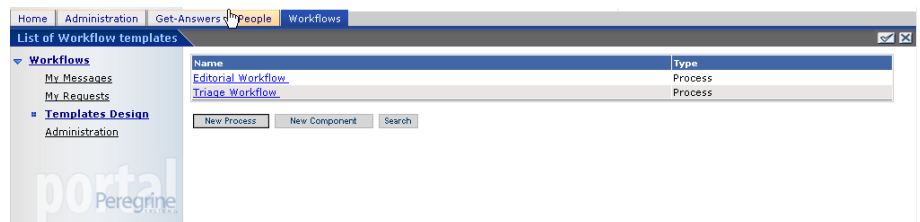
4   Click the name of the workflow template you want to modify.

The **Details for template** page appears.
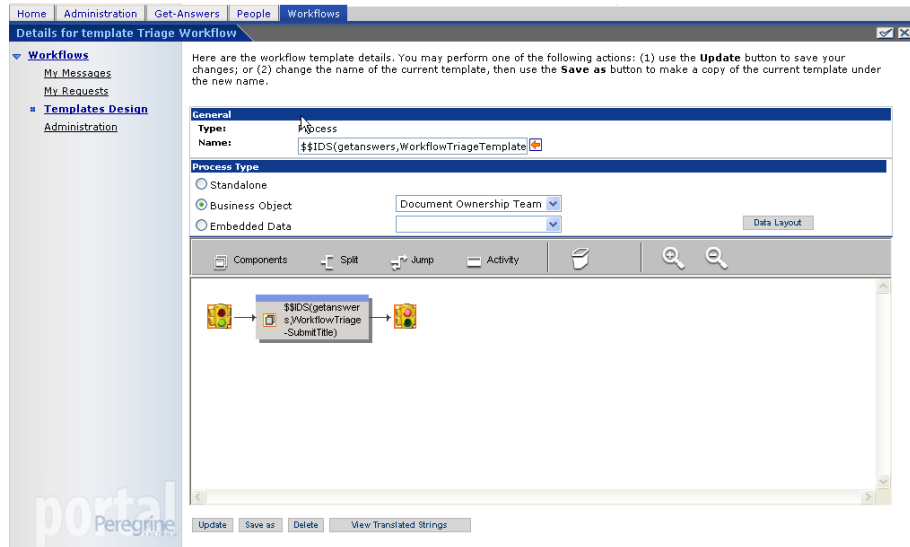
5   Make the necessary modifications to the template.

See Creating a workflow template on page 312 for information on adding, modifying, or deleting activities.

6   Click **Update** to update the workflow template and return to the **List of Workflow templates** page.

7   Click **Save As** to save your template modifications as a new template.

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 Get-Answers.

2   Click the Workflows tab, or click **Workflows** from the Navigation Menu.

    The Workflows menu appears in the left pane.

3   Click **Template Design** from the Workflows menu to display the **List of Workflow templates** page.
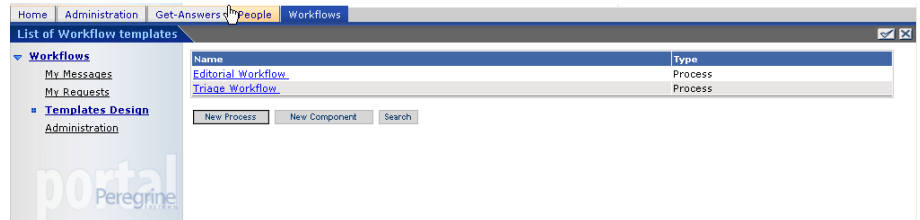
4   Click the name of the workflow template you want to delete.

    The **Details for template** page appears.

5   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 Get-Answers.

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.
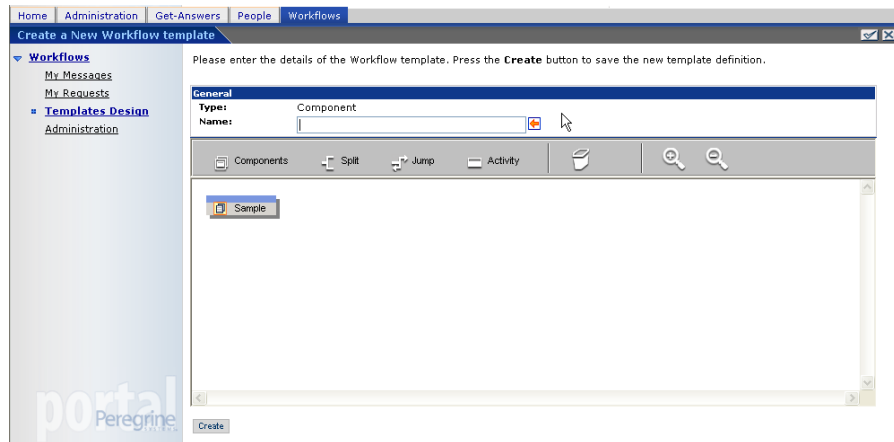
5   In the **Name** text box, type the name of the new component template.

    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 adds 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 337 and Deleting an activity on
    page 337.

6   In the workflow designer, create and add activities to the component template using the toolbar icons described in the following table.

Icon	Description
Components	Select a new activity from the template list. See To add a component template: on page 335 for information on adding an activity from the template list.
Split	Create a new Select activity. See To create and add a Select activity: on page 329 for information on adding a Select activity.
Jump	Create a new Jump activity. See To create and add a Jump activity: on page 332 for information on adding a Jump activity.
Activity	Create a new activity. See To create and add a new activity: on page 316 for information on adding a new activity.
	Trash. See To delete an activity: on page 338 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 316. To create and add a Jump activity, see Creating a Jump activity on page 332. To create and add a Select activity, see, Creating a Select activity on page 328. To add a component template for inclusion into this component template, see Adding a Component Template on page 335.

See Modifying an activity on page 337 and Deleting an activity on page 337 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**, Workflow discards all changes to the template.

Using Workflow Administration

This section explains the functions available in Workflow Administration activity. The functions described include:

- Accessing the Administration function on page 344
- Monitoring process instances on page 345
- Updating a process instance on page 347
- Starting a new process instance on page 349
- Viewing the Event Queue on page 351
- Setting Up the Request List on page 353
- Uploading JavaScript Files on page 360

Accessing the Administration function

The workflow administration functions can be accessed only by users having the required capabilities (permissions).

To access the Workflow Administration function:

1   Log on to Get-Answers.

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 to display the **Administration of processes**.
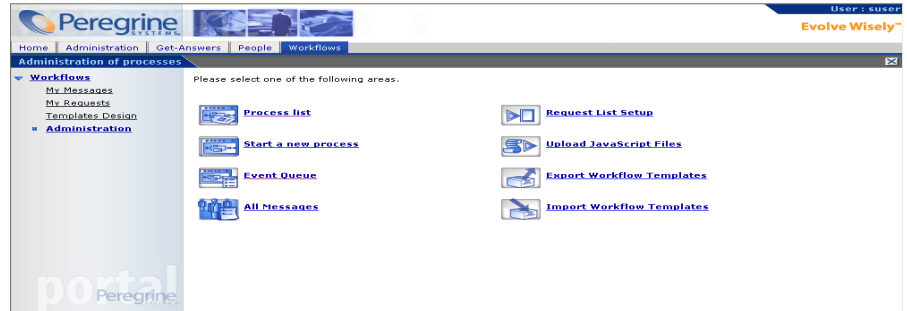
From this page you can select the following areas of administration:

■   Process list

■   Start a new process

■   Event queue

■   All Messages

■   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** pens.
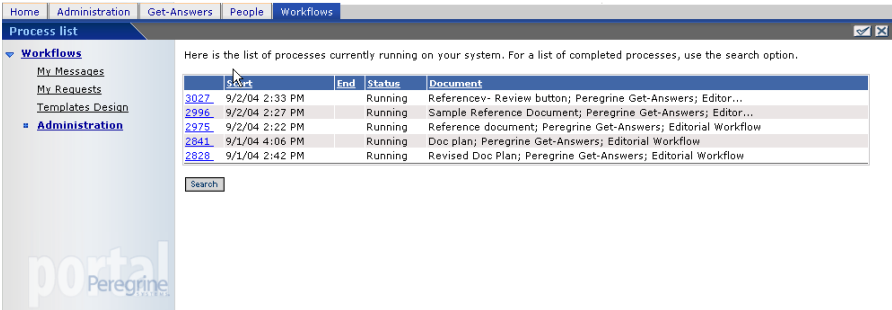
A list of all processes started in the system opens in the Process list window. The list contains the following columns of information about the associated process instance:

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—The name of the document and the process phase of document.

2   To sort the list according to a particular column attribute, click the column heading.

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.

4 Enter your search criteria in the fields provided.

5 Click **Perform Search**.

A list of the processes matching your search appears.

6 Click **Search** to begin a new 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 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 To sort the list according to a particular column attribute, click 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.
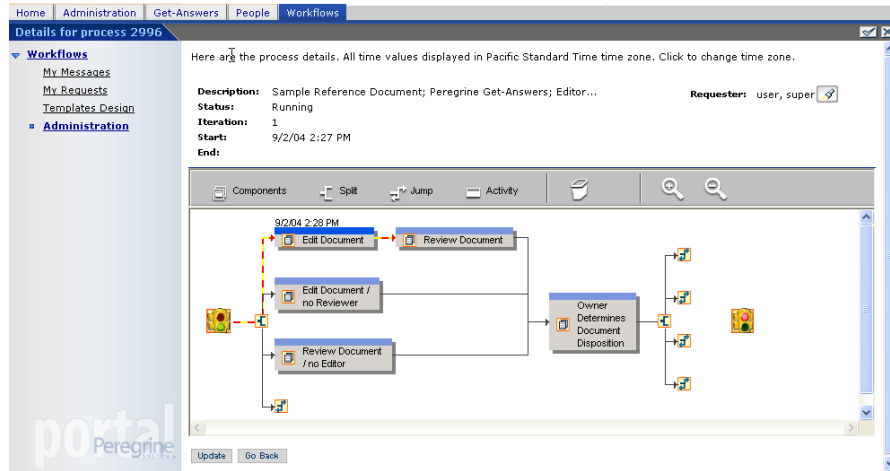
5   Make the necessary changes to the process instance activities.

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. When a process is deleted, the document is also 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.
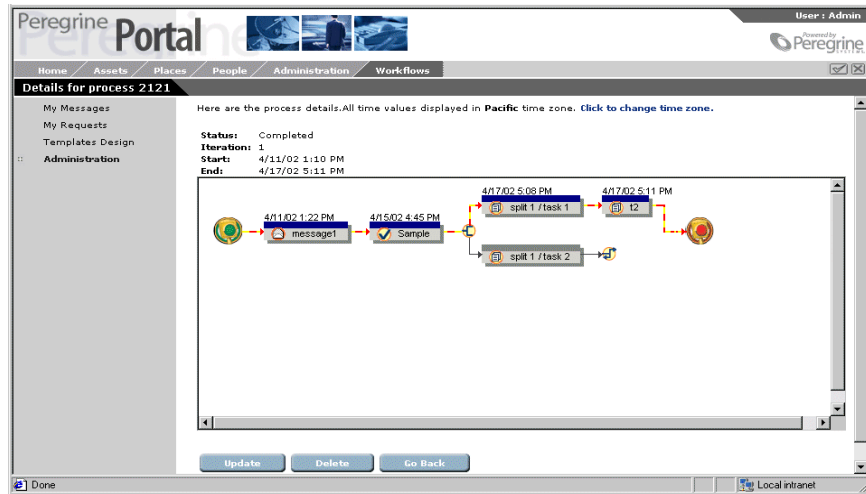
4   Click **Delete** to delete the process instance and return to the Process list
    page.

Starting a new process instance

You can manually start processes that are not related to documents 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.
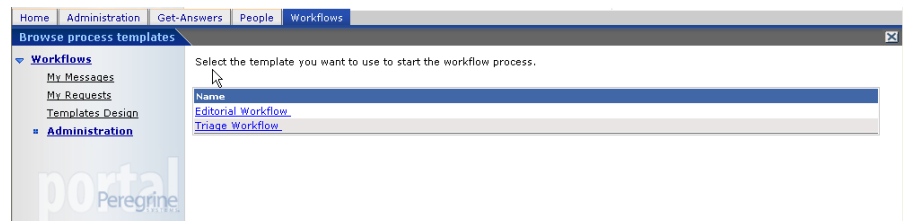
2 From the list of templates, select the template you want to use to start the workflow process.

The **Process submit** page opens.

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:

Event queue	Description
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**.
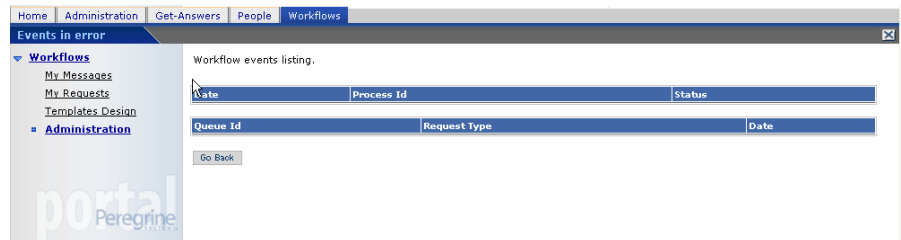
2 To view the details of an event, click any of the column entries associated with that event.

   The **Event detail** page opens.

3 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.

Using administering work messages

Administrators can use the All Messages feature to search for, view messages, and preview the associated documents assigned to any system users.

The search function lists messages by status (In Process, Overdue, and Pending Acceptance). You can limit the search by including the assignee and document ownership team for the messages.

To search for document messages:

1   From the **Workflows** page, click **All Messages**.

The User Workflow Messages page opens.
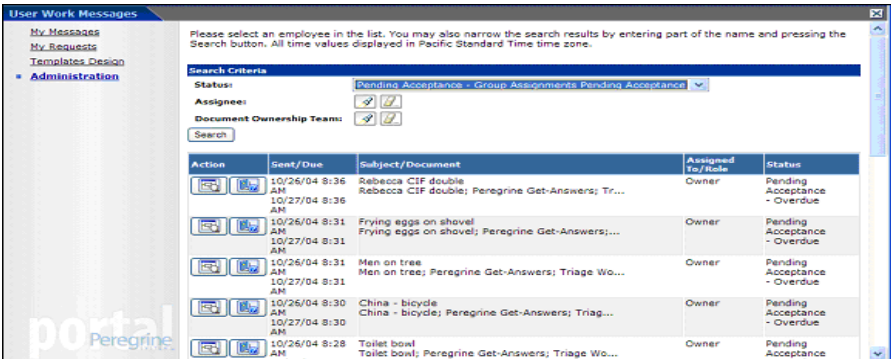
2   Provide the appropriate search criteria.

3   Click **Search**.

The User Work Messages page displays the search results.

Administrators can click the following icons to review details:

preview icon ⊞	Displays a preview of the document associated with that workflow message.
workflow icon ⊞	Opens a workflow details screen that allows the administrator to return accepted assignment to a group, or reassign the assignment to another user.

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 definitions support various request functions; however, you may need a programmer to write specific scripts to provide the functionality the request definition requires.

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, or you can use he New button to begin the creating a new workflow request. To narrow the search, provide as much information as possible.

To search for a request definition:

1   From the **Administration of processes** page (Workflow tab > Administration), click **Request List Setup** to display the **Request Search** page.

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 search icon next to Workflow Template to display the search
    window.
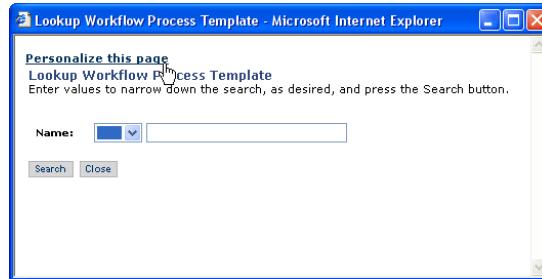
4   Using this window, locate and select the workflow template.

5   Click **Search** to filter the list of request definitions and display only those
    matching the search criteria.

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.

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 search icon next to Workflow Template to display the Lookup Workflow Template window.
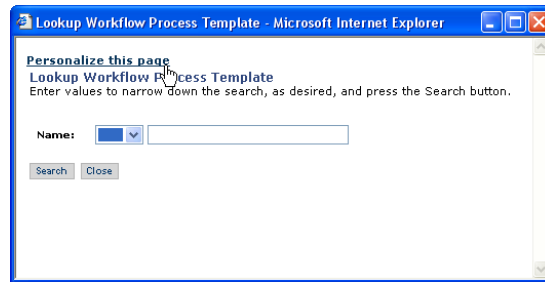
a   Using this window, define your search criteria.

b   Click **Search**.

The Lookup Workflow Template window displays a list of all workflow templates matching the search criteria.
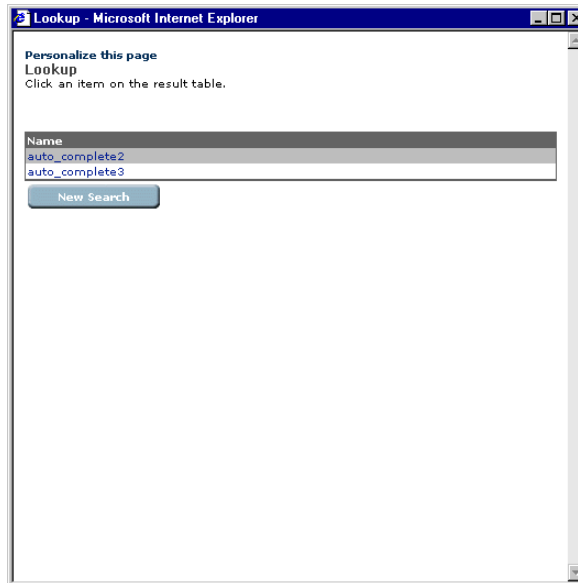
c   From the list, select the workflow template to associate with the request definition.

7   Select the **Show Startup Screen** check box if the workflow template was created as an Embedded Data process type.

See .

8   Click the search icon next to Startup Script to display the Script File Lookup window.
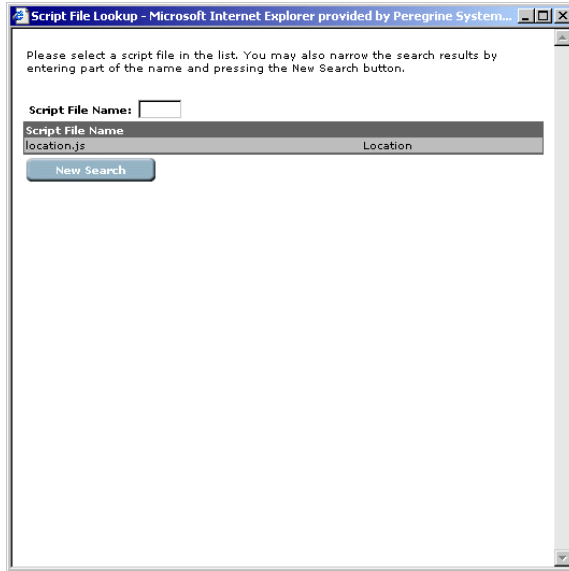
9   Locate and select the script file you want to use.

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 354 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 354 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 the 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.
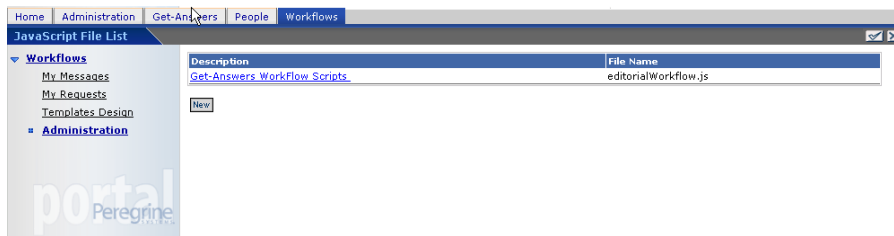
A list of all script files previously uploaded to the server appears. The list contains the following columns of information about the script file:

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.
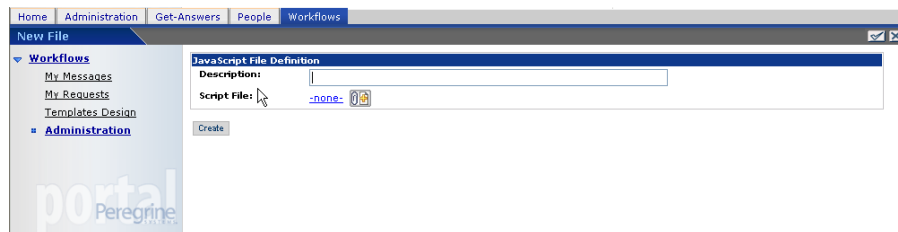
2   Type a description of the script file in the **Description** text box.

 3   Click the Plus icon to display the Select a File window.

4   Use the **Browse** button to display the Choose file window.
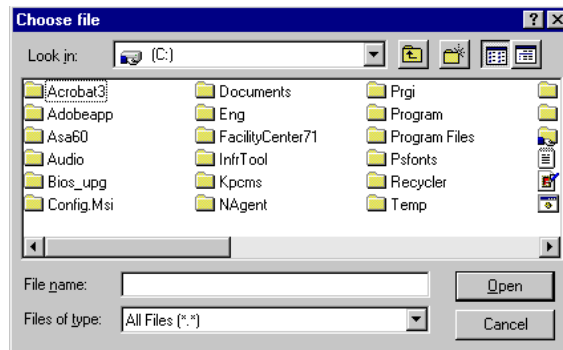
5   Locate and select the script file to upload.

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.
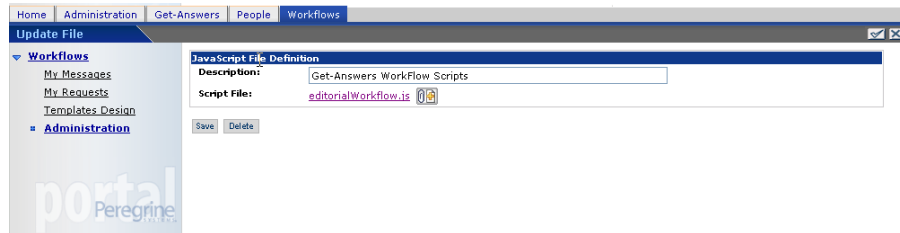
2   Make any required changes in the **Description** text box.

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.

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: /WorkflowImportExport/   ←

Next

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 be be imported.

Import File Path: /WorkflowImportExport/   ←

Document files found in import directory:
NSTemplate.xml
WfwJSFile.xml
WfwRole.xml
WfwTemplate.xml

Script files found in import directory:

Start Import   Refresh File List

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 339 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 Get-Answers.

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 steps to view the details of a request.

To view the request details:

1 In the description column of the My Request page, click the description for the request you want to review.

The detailGeneral page opens.

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 .

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 356.

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, or click **Setup Request List**.

The workflow process instance for the request appears in the request list of your **My Requests** page or you can create a new request.

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.
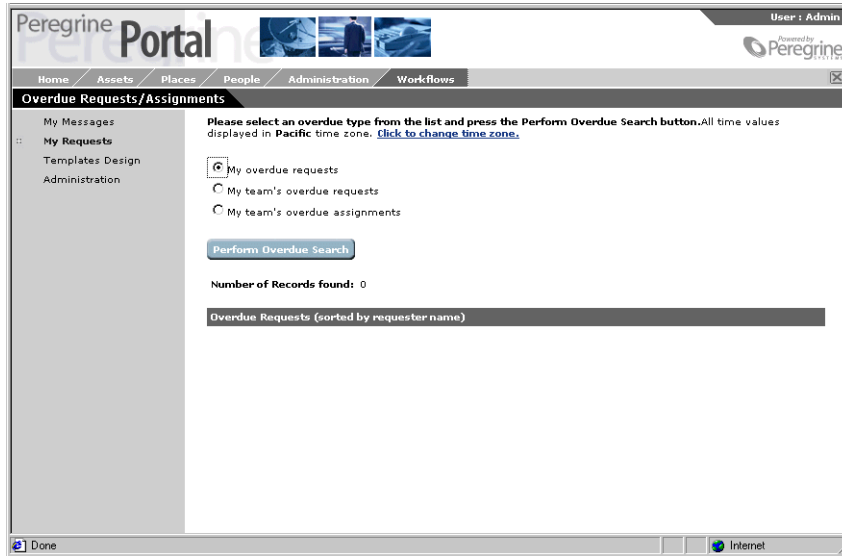
Note: Times appear according to the time set in your Change Time Zone Preference page. To change to another time zone, from the Home tab, click the **Click to change time zone** link, select a time zone, then click **Submit**.

2 Click the search icon next the 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.

Setting Up E-mail Notifications

You can set up Get-Answers to send an automatic notification to users when they have a Get-Answers Document Team task in their queue or their group's queue, such as the Get-Answers Team editor's queue. You need to have system and user administration rights to perform this task.

To setup mail notifications:

- Set up the mail adapter link.
- Import the Notifications Templates (both of them).
- Reload the plug-ins.
- Add the notification to each workflow action.
- Add E-mail addresses.
- Test E-mail notification.

Set Up the Mail Adapter Link

To setup the mail adapter link, you need provide the mail server name and the admin user's E-mail address.

To setup the mail adapter link:

1   From the `admin.jsp` page, click the **mail adapter** link.

2   Add the mail server name to the Inbound Mail Host and Outbound Mail Host fields.

3   Add the admin user's E-mail address into the Mail sender address field.

4   Click **Save**.

5   Click the **Control Panel** link of the Admin Settings menu.

6   Click **Reset Peregrine Portal**.

Importing the Notifications Templates

You must import both Notification templates to use with E-mail notifications.

To import the Notification templates:

1   From the login.jsp page, click the **Administration** tab.

2   Click the **Data Import** link in the Notification Services Administration section.

3   Click **Next**.

4   Check both rows in the table (`notificationservices_en.xml` and `workflowplugin_en.xml`).

Note: You may see others if you have localized languages.

5   Click **Finish**.

Reloading the Plug-ins

You must reload the plug-ins so that they are active.

To reload the plug-ins:

1   On the Administration tab click the **Plug-In Status** link.

     The Workflow Plug-in has the status of Inactive.

2   Click **Reload Plug-ins.**

     The Workflow Plug-in now has a status of Active.

Adding the E-mail Notification to Each Workflow Action

You must now add the E-mail notification task to the triage and editorial workflows.

To add the E-mail notification to the Triage workflow:

1   In the Workflow tab, select **Templates Design.**

2   Open the **Triage Workflow** template.

3   Click the **$$IDS** (getanswers, WorkflowTriage-SubmitTitle) box. The box is called an Action.

4   Click **Next.**

5   Check the **Notify assignee** of this task check box.

6   Click Next.

7   Click **Update** for the wizard.

8   Click **Update** for the template.

To add email notification to the Editorial workflow:

1   Open the Editorial workflow template.

2   For each of the Actions (by default there are five of Actions here):

   a   Click the action.

   b   Click **Next.**

   c   Check the Notify assignee of this task check box.

   d   Click **Next**.

   e   Click **Update** for the wizard.

3   Once each action is updated, click **Update** for the template.

Adding E-mail Addresses for the Users

For each user that is either an Owner, Editor, or Reviewer on a Document Ownership Team, add their E-mail address to the E-mail collections. Make sure they have a primary E-mail account.

To add E-mail address for the users:

1   Click the **People** tab.

2   Click **View All** or search for the user whose profile you want to edit.

3   Click the name of the user for whom you are adding an E-mail address.

Note: If E-mails is not showing on the people edit/ people create page, personalize the page to add it.

4   In the E-mails section of the people edit page, click **Add** to open Create New Person Email window.

5   In the Email Type field, select primary and type the user's E-mail address in the Email field.

6   Click **OK**.

7   Click **Submit Changes**.

8   Repeat steps 2-7 for each person whose E-mail address needs to be added.

Testing E-mail Notification

After you have setup E-mail notification, you should test it to ensure that the E-mails are being sent correctly.

To test E-mail notification:

1   On the Portal Page, click **Send Notification**.

2   Click **Add**.

3   Select a user (or users).

4   Set Device to E-mail.

5   Type "Notification Test" in the Subject line.

6   Type "Please respond to this email by clicking yes. Then click Submit" in the Text field.

7   Type "Did you receive this?" in the Question field.

8   Click the **Send** button.

9   Verify that the user(s) received their E-mail and have the user(s) respond to the E-mail.

10   Verify that you received the response on your Check Inbox screen.

     If you did not receive a response or if a user did not receive an E-mail, review the procedures for setting up automatic notification and make any changes required.

11

CHAPTER

Document Types and Views

This chapter describes how to work with Document Types and Document Views. The topics covered in this chapter are:

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, Reference, Error Message/Cause 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 the information displays 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 view the same documents, but only those users with certain permissions can view 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.
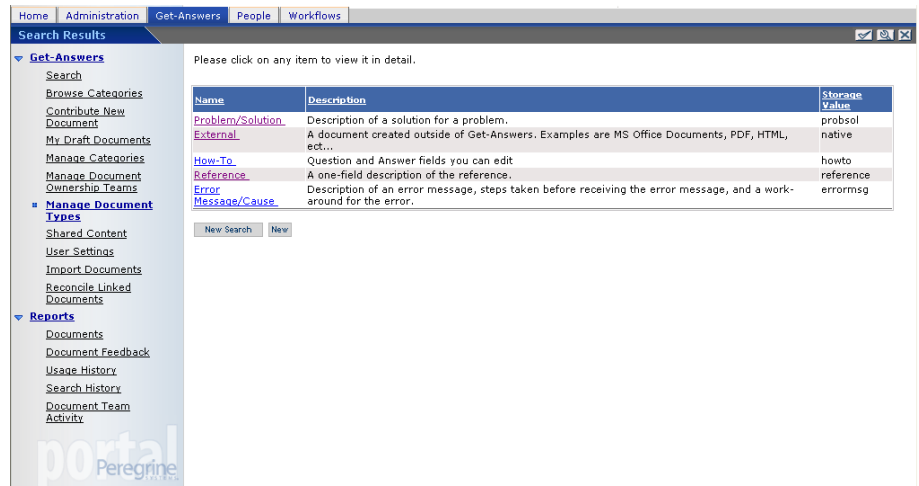
Adding a view to a document type

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**.

4   A search page opens.

5   Enter the search parameters and click **Search**, or click **View All**.

A list of document types appears.

6   Click document type you to which you are adding a view.

The Document Type Details window opens.

7   Enter a name for the view, for example, Sample ProbSol View.

8   Continuing with the example, enter sampleprobsol 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.

9   Enter a description of the example, such as, "Sample Problem/Solution view."

10 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.

11 Enter a name for the view, for example "Sample Problem/Solution view."

12 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 available for everyone. You cannot have the same security level for every document view of the document type.

13 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.
Checked Out By	Not presently used; available for customer use.
Creation Date	The date that document was added to the system, e.g., 2003-5-11.
Attached files	
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	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.
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.
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.
Published	Published status of the document, either 'Published' or 'WorkingCopy.'
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.

Field Name	Description
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.

14 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 User's Guide for more information about the edit-on Pro features for formatting text.

15 Continue adding fields on the form using the Field List drop-down and Insert Selected At Cursor.

16 You can also use the buttons in Add Content Choices to add additional content to the new document view. The buttons are:

Button	Description
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.
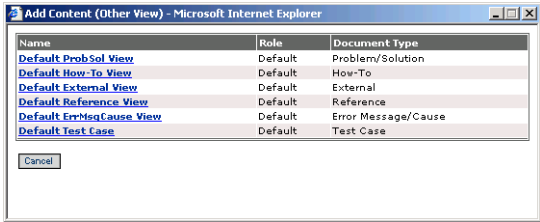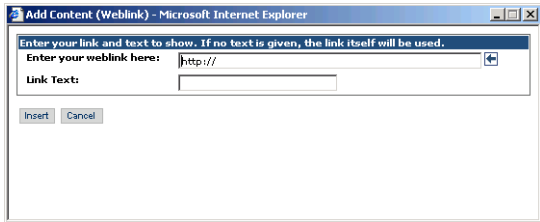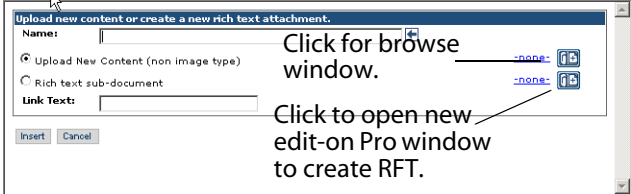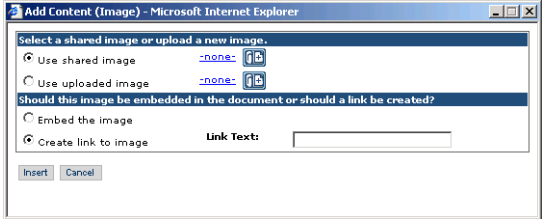
Button	Description
New Upload	Use this button to add an external attachment. The attachment is usually a Word document, txt file, PDF file or some other type of external document. Because this document is an attachment, it is not included in the index and does not appear in any search results.
	You can 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 RFT 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.

17 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.

Note: On Netscape/Mozilla if you add a Role to a DocView AFTER you have made changes to the View data in the RTF Editor, the View data changes are lost. As a workaround in Netscape 7.1 under Manage Document Types, when creating or modifying a document view, add roles before adding new fields to the view or modifying the view, so that view changes are not lost.

To add a role to a document type view:

1 From the Get-Answers tab, click **Manage Document Types**.

A search page opens.

2 Enter the search parameters and click **Search**, or click **View All**.

A list of document types appears.

3 From the list, click the name of the document type.

The Document Type Details page opens.

4 In the Document Views section, click the document view to which you are adding a role.

The Document View Details window opens.

5 Click **Add** next to Roles.

A Roles search window opens.

6   Click the search icon.

The Lookup Roles window opens.

7   Enter the search parameters or click **Search**.

The Lists of Roles window opens.
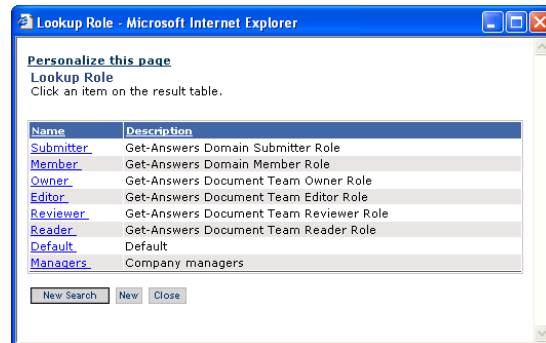
8   In the list, click the role you are adding to the view.

The Roles window opens with the role you selected listed.

9   Click **OK**.

The Document View Details window opens with the role you selected listed in the Roles section.

10   Click **Submit View Changes**.

The document view is now available for users assigned to the role you added to the view.

Adding a new document type

Get-Answers comes with a set of default document types, but you can add additional document types. You also need to add additional document types if you migrate documents from Knowlix, which may include documents types not available in the set of default document types.

To create a new document type:

1   Log in to Get-Answers.

2   From the Peregrine Portal, click **Get-Answers** tab.

3   Click **Manage Document Types link**.

A search page opens.

4   Click **New**.

The Create New document type page opens.

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 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 systems comes with a set of document types which are be 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.

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 you personalization changes and close the window.

5   Click **Preview Document** to view your changes.

6   Click 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 appears in the edit form you created.

12

CHAPTER

Importing Legacy Data

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 394 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 legacy data on page 394 for more information.

Once you have converted your data, use Get-Answers to import it to the Get-Answers database. SeeConverting legacy data on page 394 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 11, 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 11, 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 legacy data on page 394.

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 into Get-Answers on page 411. 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 <u>any</u> 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.
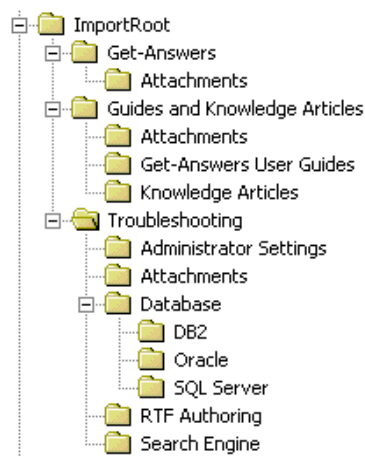
Each subfolder under a top-level category folder such as Troubleshooting will be created as a subcategory during the Import Document processing. In the example above, the top-level category named Troubleshooting has four subcategories, and Troubleshooting's subcategory named Database has three subcategories.

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 must create the document ownership teams to maintain the new documents that you are importing before you import. See Categories and document ownership teams in Chapter 2, Setting-up Get-Answers for more information about adding categories and document ownership teams. Import the documents for one document ownership team at a time. When you are ready to import documents, see for the steps to follow to import your documents.

Once you have imported, you cannot change the team that manage 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   The `.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 11, 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
<?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/oaa/login.jsp) instead of
http://localhost/oaa/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 pre-defined fields supported. Pre-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. You may wish to store some of your own fields in the database rather than in the BLOB field. This allows the fields stored in the database to accessed withe SQL queries for reporting functions. See Sample schema extensions for Get-Answers on page 177 in Chapter 6, Schemas.

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
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 To create a new document view: on page 377.	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

Field/XML Tag	Description	Max Number of Bytes
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 following is an example of a company-generated .xml authored document.

```xml
<?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>
         <p align="left">This is a font <font face ='Courier
            New'>change</font></p>
        <p align="left"></p>
            #0000FF></font></p>
        <p align="left">This is a bulleted list:</p>
        <p align="left">&#149;   line 1</p>
        <p align="left">&#149;   line 2 </p>
        <p align="left">&#149;   line 3</p>
        <p align="left"></p>
        <p align="left">This is a numbered list</p>
        <p align="left">1.   line 1</p>
        <p align="left">2.   line 2</p>
        <p align="left">3.   line 3</p>
        <p align="left"></p>
        <p align="left"></p>


    ]]>
```

```
        <p align="left">This is a font size <font size
=5>change</font></p>
        <p align="left"></p>
        <p align="left">This is a font color <font color =
            #0000FF>change</font></p>
        <p align="left"></p>
        <p align="left">This is a font face, color and size <font
face ='Courier
            New'>
          <font size =5><font color =
                    #0000FF>change</font></font></font></p>
        <p align="left"><font color = #0000FF></font><font color
=
   </Solution>
   - <AuthorName>
      - <![CDATA[ jsmith  ]]>
   </AuthorName>
   - <KnowlixDocument_ID>
      - <![CDATA[ S97-M18-PZSW  ]]>
   </KnowlixDocument_ID>
   - <History>
      - <![CDATA[
         "08/26/2003 11:51:36","jsmith","Created"
         "08/26/2003 11:58:43","jsmith","Modified"
         "08/26/2003 11:58:47","jsmith","Approved: Initial"
         "08/26/2003 11:58:53","jsmith","Copied to Smoke Test NFO"


      ]]>
   </History>
   - <JumpDestination>
      - <![CDATA[   ]]>
   </JumpDestination>
   - <OwnedDocs>
      - <![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 406 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 underscorcs (_) 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.
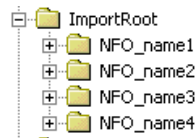
Importing your data into Get-Answers

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.

Note: You must create a document ownership team to maintain the new documents you are importing. You should do imports so that you only import documents for one document team at a time.

Before you can import xml files you need to ensure that these files have valid characters in them for the character set specified. The character set is indicated in the first line of the xml file.

```
<?xml version="1.0" encoding="ISO8859-1" ?>
```

You can view the xml file in a text editor and change the file content type header to ISO-8859-1 or you can use the save as feature of some text editors to convert the file to a UTF-8 character set (Notepad is able to Save As UTF-8).

To import converted documents into Get-Answers:

1   Move the data you have converted to a directory on the Get-Answers application server.

2   Log on to 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.

5   On this page:

     a   Type, in Import Document Root Path, the directory path for the location of the documents you are importing. (Required entry)

       The path you enter should be one directory above the top-level category directory for that team. For example, if you have a top-level category named Get-Answers and a directory named Get-Answers that contains the files and the attachments directory for the Get-Answers top-level category,

```
C:\Program Files\Peregrine\Common\
Tomcat4\webapps\oaa\integrations\ImportRootExample\Get-Answers
```

you should enter the following path for Import Document Root Path.

```
C:\Program Files\Peregrine\Common\
Tomcat4\webapps\oaa\integrations\ImportRootExample
```

   b   In the Document Ownership Team field, choose a document team to
       manage the documents.

   c   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).

   d   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."

   A message box also displays a message directing the user to restart the
   application server if the schema was extended.

Important: After all of the documents are imported, you should restart the
            application server if you extended the rKmDocument schema. After
            you restart the server use the Reconcile Linked Documents function
            to run the Link Management Utility.

Managing migrated documents

To manage documents migrated from Knowlix, follow these steps:

- 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. To set document ownership team permission, see Managing categories and document ownership teams on page 55 in Chapter 2, Setting-up Get-Answers.

Use the Set Security Capabilities page to update the security capabilities. To update the security capabilities of a user, see Working with document ownership teams on page 55 in Chapter 2, Setting-up Get-Answers

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 Extending schema extensions in Get-Answers on page 170.) 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 and edit form for the new document types created during the migration process.

Note: See Chapter 11, Document Types and Views and Chapter 5, Personalization for additional information.

To create a new input 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.

This page probably does not have the fields that authors or editors 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. You should see the new fields that became available because of the new documents you migrated from Knowlix.

Use the information gathered from KnowlixAuthor (Preparing for the conversion from Knowlix on page 409) 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 to Document Views.

4   Use the field names in the field list to add them to the view.

See Chapter 11, Document Types and Views for adding fields to the document view.

5   Click **Add New View** to save the view you created.

Removing like-named document types

It is possible that the sample document types supplied with Get-Answers include document types names exactly the same as document types in Knowlix.

Warning: 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 11, Document Types and Views for information about deleting document types.

Updating 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 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"`.
   e   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 .

A Troubleshooting Get-Answers

APPENDIX

This appendix describes the problems that may occur after installing Get-Answers and their solutions.

Troubleshooting errors

Missing workflow messages or receiving duplicate messages

There is a configuration problem with the web application when users are either missing workflow messages or receiving duplicates of them.

To correct this problem:

- Ensure that all of the properties set on the various tabs on the Admin Setting page are correct. In particular, ensure that the Enable script pollers property on the Common tab is set to **Yes**.

- Ensure that the Event queue property on the Common tab is set to **rome**.

To find missing workflow message:

1   Log on to Get-Answers as an administrator.

2   Click the Workflows tab.

3   Click the Administration menu item.

    The Administration of processes page opens.

4   Click the Event Queue.

The Events in error page opens.

5   Verify that there are no processes with an Error status.

6   If a process appears with an Error status appears, click the process.

7   Read the error message that appears and correct the circumstances that caused the error.

8   Click the **Update for processing** button to re-submit the workflow message.

When workflow messages are missing for Get-Answers assignments, one possibility is that no owner was found within the documentation team when Workflow tried to resolve the role assignment. You can use the Event Queue option. (see attached images, John)

1   Log on to Get-Answers as an administrator.

2   Click the Workflows tab.

3   Click the Administration menu item.

The Administration of processes page opens.

4   Click the Event Queue.

The Events in error page opens.
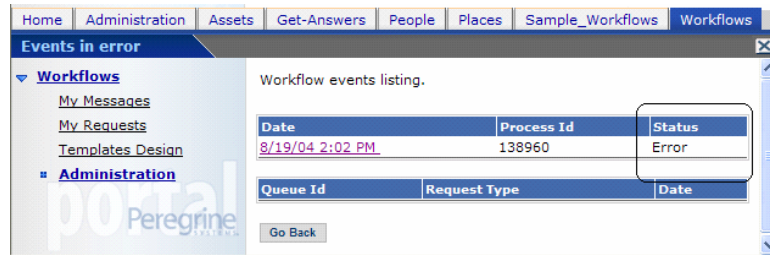
If there is an event with an error status, you can click that event to view details. If no one is found during the role assignment process, you should see an error similar to the following.
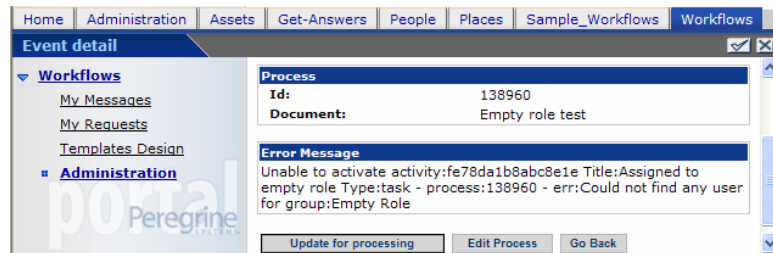
Error Message: Unable to activate activity:fe78da1b8abc8e1e Title:Assigned to empty role Type:task - process:138960 - err:Could not find any user for group:Empty Role

5   If this is the case, make sure that there is at least one member in that role within the doc team to receive the assignment. A functional role is a group of users under the People tab. In Get-Answers, a functional role can be a document team Owner, Editor, or Reviewer. That functional role may not have any users in it, and a document ownership team with no owners is not functional. Submitters will contribute new documents and no one will review and publish the documents. Those documents will be in an Error status in the Workflow Event Queue.

For example, if the error text reads:

```
...Could not find any user for group HR Managers
```

There is a functional role (group of users) such as 'HR Managers' as the owner of a document team, and it appears to be empty.

6 Navigate to the People tab to ensure that 'HR Managers' has at least one user in that Functional Role.

   a Click **People** tab.

   b Click the **Functional Roles** menu link.

   c In the list of function roles that appears, click the role for which no users are found. In this example, you would click HR Managers.

   d In the Roles detail page you should find that there are no users defined for this role.

   e If there are no users, use the wrench icon in the upper-right corner to customize the Role Details page to add the collection of users to the details page. For a detailed explanation of personalization, see Chapter 5, Personalization.

7 To personalize the page and add a user or a collection of users:

   a Click the wrench icon on the Role Details page.

   b In the Personalize Document Detail page, add People to the Current Configuration list.

   c Click **Save**.

      You should now have a People label in the Role Details page with and Add link.

   d Click the **Add** link, to add a user or group of users to this role.

8 Now you can go back to the Workflow Admin page to display the event and use the **Update for processing** button to re-submit the workflow message to the Workflow engine.

Glossary

This glossary contains general terms used when describing Get-Answers, OAA platform, and Workflow.

Term	Definition
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.

Term	Definition
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

Term	Definition
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.

Term	Definition
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 Organizational Role).
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.

Term	Definition
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	A process definition represents a business process and consists of activities where the process tasks are defined.
	A process definition includes information about the activities and workflow users. Both manual activities and automated activities can be included in the process definition.

Term	Definition
Process instance	A single instance of a process as defined by the process definition. A process that has been started is a process instance.
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	A representation of the status of a process instance. The Get-Answers workflow uses the following process states: **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. Readers can view unpublished 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.

Term	Definition
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 lifestyle 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	A software service or "engine" that provides the run time execution environment for a process instance. The workflow engine interprets the process definition, creates process instances and manages their execution, and navigates activities and creates work items for their processing.
Workflow participant	A user that performs the work items assigned through the worklist. Each work item is represented by a workflow activity.
Working copy	Working Copy is a version of the published document in an editorial status.
Worklist	A list of work items associated with a specific user or group of users.
XML	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.

Index

PEREGRINE