Peregrine

Get-Services 4.0

Administration Guide

For Windows, AIX, Linux, and Solaris

PART NO: GET-SER-4.0-ENG-01029-00250

Peregrine SYSTEMS®

If you need technical support for this product, or would like to request documentation for a product for which you are licensed, contact Peregrine Systems, Inc. Customer Support by e-mail at support@peregrine.com.

If you have comments or suggestions about this documentation, contact Peregrine Systems, Inc. Technical Publications by e-mail at doc_comments@peregrine.com.

This edition applies to version 4.0 of the licensed program.

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

Contents

About this Guide

Get-Services is an application that provides a web-based interface to Peregrine ServiceCenter®. Get-Services allows users to report and track problems in their work environment by opening tickets.

This guide explains the concepts of the Get-Services interface. Information includes:

- Performing administrative tasks in Get-Services
- Configuring Get-Services for ServiceCenter
- Understanding how users are identified in Get-Services
- Using the Peregrine Portal
- Personalizing forms

Book audience

This guide is intended for administrators who configure and maintain Get-Services. To use this guide effectively, you must have a working knowledge of the following:

- XML and ECMAScript (or JScript/JavaScript)
- Operating guides, reference manuals, and other documentation for your PC hardware and operating system
- ServiceCenter administration and functionality

Related documentation

Refer to the following documentation for additional information:

This manual…	Provides information on…
Get-Services Installation Guide	installing and configuring the Peregrine OAA platform, Get-Services, Java SDK, and application and Web servers.
Get-Services Release Notes	any late- breaking documentation or known issues with Get-Services. These are constantly updated and posted to the Customer Support web site. See *Contacting Customer Support* on page 10 for details on accessing the Customer Support website.

Associated applications

This guide does not contain information about products that may be used with Get-Services, such as ServiceCenter or Password Management. Refer to the appropriate product documentation for information about installing, configuring, and using these associated applications.

Note: You must install and configure ServiceCenter before you can install and configure Get-Services. Refer to the *Get-Services Installation Guide* for instructions.

Terminology

The terminology used in this guide and in the Get-Services interface is based on ServiceCenter 4.x and 5.x.

Typographical conventions

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

Convention	Meaning
Bold	Information that you must type exactly as shown appears in **bold.** The names of buttons, menus, and menu options also appear in **bold.**
Italics	Variables and values that you must provide appear in *italics*. New terms also appear in *italics*.

`Monospace`	Code or script examples, output, and system messages appear in a `monospace` font.
	`var msgTicket = new Message( "Problem" );`
	`...`
	`msgTicket.set( "_event", "epmc" );`
	An ellipsis (...) is used to indicate that portions of a script have been omitted because they are not needed for the current topic. Samples of code are not entire files, but they are representative of the information discussed in a particular section.

Sans Serif	Filenames, such as login.asp, appear in a sans serif font.

Special elements

This book uses special elements to help you locate information. These special elements and their uses are 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 following table shows you where in this guide to find the information you need.

To find this …	Look here…
Peregrine OAA architecture overview	*Chapter 1, Architecture Overview*
Get-Services features and architecture overview	*Chapter 2, Get-Services Overview*
Customizing the Get-Services interface	*Chapter 3, Customizing the Peregrine Portal*
Configuring and using the Peregrine Portal	*Chapter 4, Using the Peregrine Portal*
Activating and using end user interface personalization	*Chapter 5, Using the Personalization Interface*
Administering Get-Services using the Admin module	*Chapter 6, Get-Services Administration*
Configuring Get-Services to work with ServiceCenter	*Chapter 7, ServiceCenter System Administration*
Security features	*Chapter 8, Security*

Contacting Customer Support

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

Peregrine CenterPoint Web site

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

http://support.peregrine.com

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

To contact Peregrine customer support

1 Log in to the Web site with your login user name and password.

2 Click **Go** beside the CenterPoint support area.

3 From **Contents** on the left, select **Whom Do I Call?** to display the **Peregrine Worldwide Contact Information**.

Documentation Web site

A complete listing of the available documentation is on Peregrine's CenterPoint Web site at:

http://support.peregrine.com

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

CHAPTER

1 Architecture Overview

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

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

Get-It Product	Description
Get-Answers™	Web-based knowledge management solution for IT that delivers a single, integrated application designed for your service desk technicians, as well as the employees you serve.
Get-Resources™	Web-based solution that integrates with AssetCenter Procurement 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 which allows employees to address their IT service requests on-line. Provides a simple interface on your corporate intranet that employees can use to report a problem, check status, request help and reset a password.

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

The base of Peregrine OAA Platform includes:

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

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

- Adapters—enables connection to the back-end system database. The adapter required by your Web application is deployed during the installation.
- OAA Persistence—provides a general purpose database that is used by certain Peregrine Web applications. OAA Persistence provides data persistence to a database.
- OAA Workflow—enables workflow capabilities used by some Peregrine OAA Platform Web applications.
- Notification Services—a centralized service for sending and receiving notifications through multiple communication devices and for tracking the status of these notifications.

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

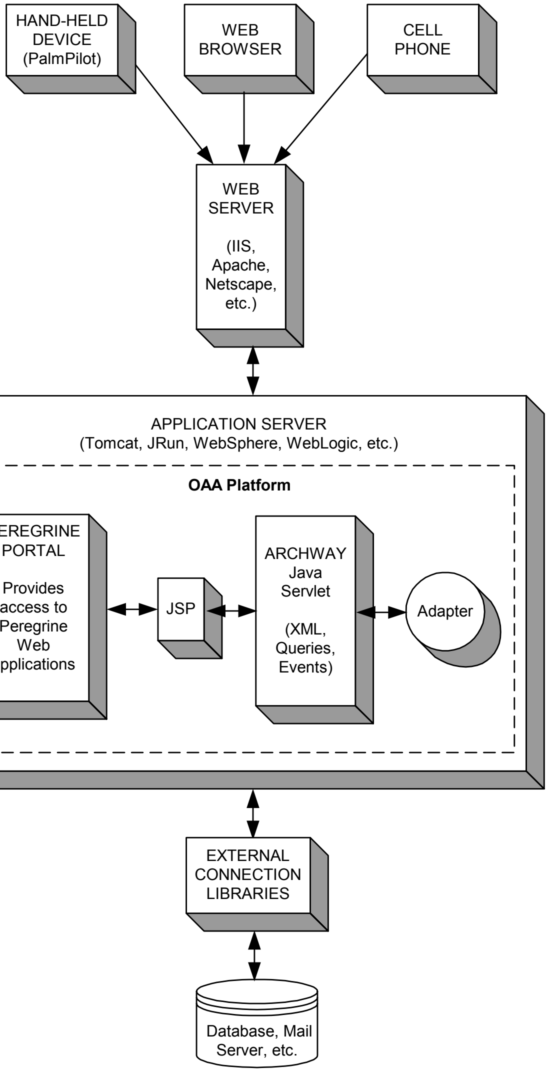
Peregrine OAA Platform architecture

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

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

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

The following diagram illustrates the architecture:


HAND-HELD DEVICE (PalmPilot)
WEB BROWSER
CELL PHONE
WEB SERVER
(IIS, Apache, Netscape, etc.)
APPLICATION SERVER
(Tomcat, JRun, WebSphere, WebLogic, etc.)
OAA Platform
PEREGRINE PORTAL
Provides access to Peregrine Web applications
JSP
ARCHWAY Java Servlet
(XML, Queries, Events)
Adapter
EXTERNAL CONNECTION LIBRARIES
Database, Mail Server, etc.

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

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

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

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

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

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

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

Archway internal architecture

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

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

Requests can be handled in one of three ways:

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

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

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

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

Each form displayed by a Web application using Peregrine OAA Platform has a related JSP. A virtual directory tells the URL the location of the JSP pages the Web browser will use to display the Web application forms.

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.

An HTTP connection consists of:

- A client request
- A server response

The messages exchanged normally have a number of header lines and some content lines. For example, consider the following two principal parts of a request:

Query String — The parameters sent with the URL for the HTTP connection.

For example:
`http://prgn/servlet/archway?hello&world`

This URL is made up of a server locator (`http://prgn/servlet/archway`) and a query string (`hello&world`).

Content — The data appended to the request. This data can be in any format, but for Archway, the data is always formatted as XML.

Archway uses the query string of a request to determine what it has been asked to do. The following query string syntax is expected:

```
archway?target.command&param=value&param=value&...
```

Consider each part of the request:

Target — The name of the target object that should handle the request. Archway forwards requests to a system and returns the response. Thus, the target could be ServiceCenter, AssetCenter, or another database. The target may also be the name of a Script Object that contains customizable logic for handling the request.

Command — The action that the target object should take. By default, five basic actions are supported: query, update, insert, delete, and event. However, when the target is a Script Object, the action can be any function defined by the script.

Param=Value — Parameter values included in the request. An arbitrary number of parameters can be passed along with the request. The encoding of these parameters is the same as that used by CGI (Common Gateway Interface). As with CGI, data sent by a browser is provided by fields embedded in an HTML form. This data is automatically formatted as a CGI request in a way that Archway understands.

The following are sample URLs that query Archway with HTTP requests. These queries return data in XML documents.

- `host name/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.

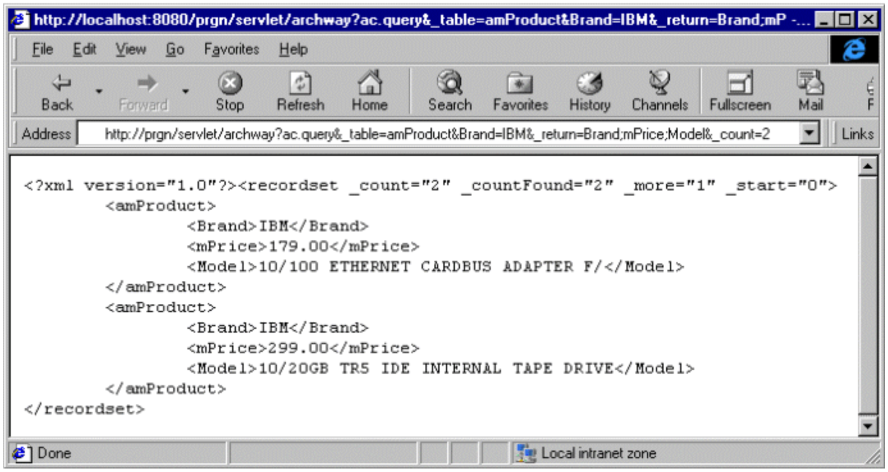
- `host name/servlet/archway?ac.query&_table=amAsset&_return=Brand;mPrice;Model&_count=2`

  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.

- `host name/servlet/archway?test.helloWorld&greeting=Hello`

  This sends a *helloWorld* request to a script object named *test*.

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



Address http://prgn/servlet/archway?ac.query&_table=amProduct&Brand=IBM&_return=Brand;mPrice;Model&_count=2

```
<?xml version="1.0"?><recordset _count="2" _countFound="2" _more="1" _start="0">
        <amProduct>
                <Brand>IBM</Brand>
                <mPrice>179.00</mPrice>
                <Model>10/100 ETHERNET CARDBUS ADAPTER F/</Model>
        </amProduct>
        <amProduct>
                <Brand>IBM</Brand>
                <mPrice>299.00</mPrice>
                <Model>10/20GB TR5 IDE INTERNAL TAPE DRIVE</Model>
        </amProduct>
</recordset>
```

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.

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 CHAPTER

Get-Services Overview

Get-Services is part of the Peregrine Employee Self Service (ESS) suite of applications built on the Peregrine OAA platform. Get-Services enables users to report problems in their work environment by opening call or incident tickets in the ServiceCenter back-end system. ESS applications empower employees to use services directly through a corporate intranet via Web browsers. The user interface is role-based and you can tailor it to meet your needs.

Topics in this chapter include:

- *Get-Services features* on page 24
- *Get-Services architecture overview* on page 28

Get-Services features

Get-Services 4.0 is compatible with ServiceCenter 4.x and 5.x. Depending on capability access, Get-Services is available to employees and technicians (IT employees). End users can create, update, and track their own tickets. IT employees can manage their own tasks using Incident Management, Service Management, and Change Management.

User roles

Users are assigned capabilities that help users accomplish their tasks. Users are the people who use Get-Services. Capabilities are the rights or permissions that users have as they work in Get-Services (see *ServiceCenter capability words* on page 99 for a listing of the capability words). This section describes users and their roles.

Get-Services defines four types of user roles: Admin, Employee, IT employee, and IT manager.

User roles	Description
Admin	Has access to the module that defines the settings for Get-Services and Peregrine OAA administration.
Employee	Creates call tickets when Service Management is enabled. When not enabled, employees create incident tickets. Employees can view, update, and close their own tickets.
IT employee	Has the same capabilities as employee, in addition to viewing unassigned tickets. IT employees can assign tickets to themselves.
IT manager	Has the same capabilities as IT employee, in addition to updating and closing all tickets.

Using the Admin module, administrators determine which user roles can reassign tickets and whether employees have Service Management enabled.

Ticket types

Incident Management is called Problem Management in ServiceCenter versions prior to 4.x. Some parameters in Incident Management use *problem* terminology because they are mapped to *problem* tables in ServiceCenter.

Get-Services has two main types of tickets: call and incident (problem).

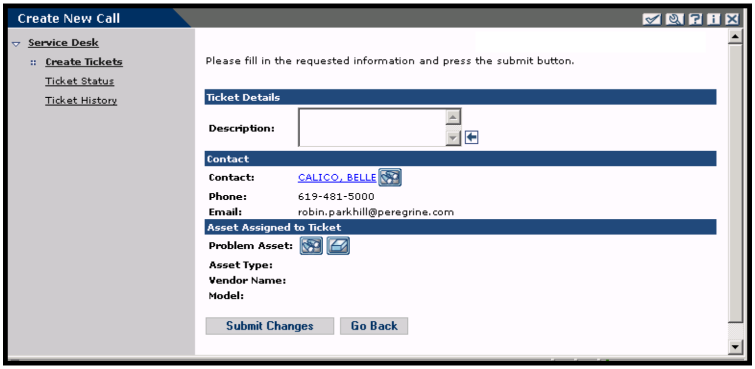
Ticket type	Definition
Call	A request for service or information. In ServiceCenter, a call is a means of establishing a line of communication with the service desk. A call report or incident ticket can be generated from a call to the help desk.
Incident (problem)	Any event that requires management beyond the standard operation of the help desk and which causes or may cause an interruption to or reduction in the quality of service.

Service Desk

Employees open tickets when they need help with any problem in their work environment. A ticket opened in Get-Services is then stored in the ServiceCenter database and is viewable from Get-Services and ServiceCenter.

Employees can view, update, and close tickets from Get-Services. The revised ticket is then updated in ServiceCenter.

Employees see only their own tickets.



Please fill in the requested information and press the submit button.

Ticket Details

Description:

Contact

Contact: CALICO, BELLE

Phone: 619-481-5000

Email: robin.parkhill@peregrine.com

Asset Assigned to Ticket

Problem Asset:

Asset Type:

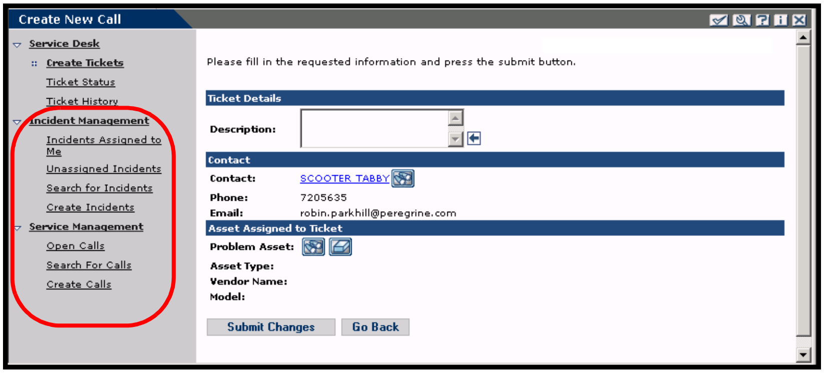
Vendor Name:

Model:

IT employees and IT managers access Incident Management and Service Management to create, update, track, and close incidents and calls. The following shows the form that opens a new ticket in Get-Services when using the ServiceCenter adapter.

Note: Service Management must be enabled (see *Configuring Service Desk parameters* on page 74) to access the Service Management options in the following graphic.

IT employees and IT Managers have Incident Management and Service Management, in addition to Service Desk.



Please fill in the requested information and press the submit button.

Ticket Details

Description:

Contact

Contact: SCOOTER TABBY
Phone: 7205635
Email: robin.parkhill@peregrine.com

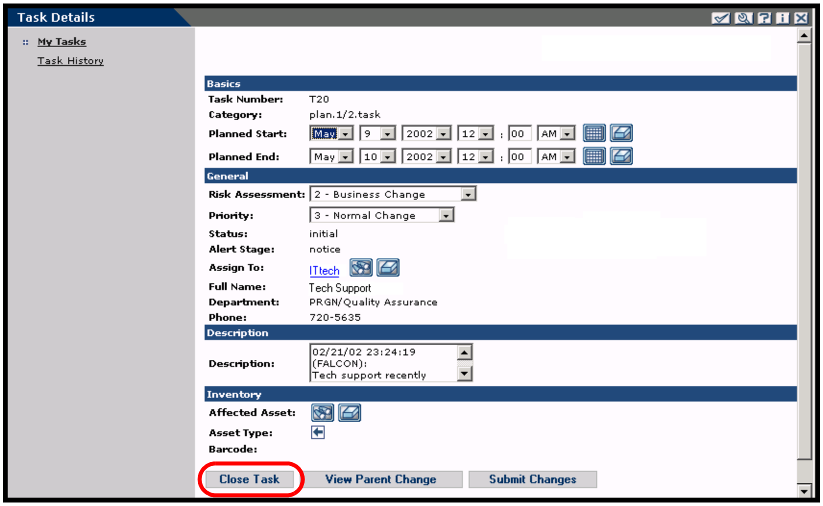
Asset Assigned to Ticket

Problem Asset:
Asset Type:
Vendor Name:
Model:

Change Management

The Change Management component of Get-Services shows field technicians their current tasks and a history of all their closed tasks. The Close Task feature is available on the Task Details form, as shown below.

Close Task is only available on the Task Details form.



Basics

Task Number: T20
Category: plan.1/2.task
Planned Start: May 9 2002 12 : 00 AM
Planned End: May 10 2002 12 : 00 AM

General

Risk Assessment: 2 - Business Change
Priority: 3 - Normal Change
Status: initial
Alert Stage: notice
Assign To: ITtech
Full Name: Tech Support
Department: PRGN/Quality Assurance
Phone: 720-5635

Description

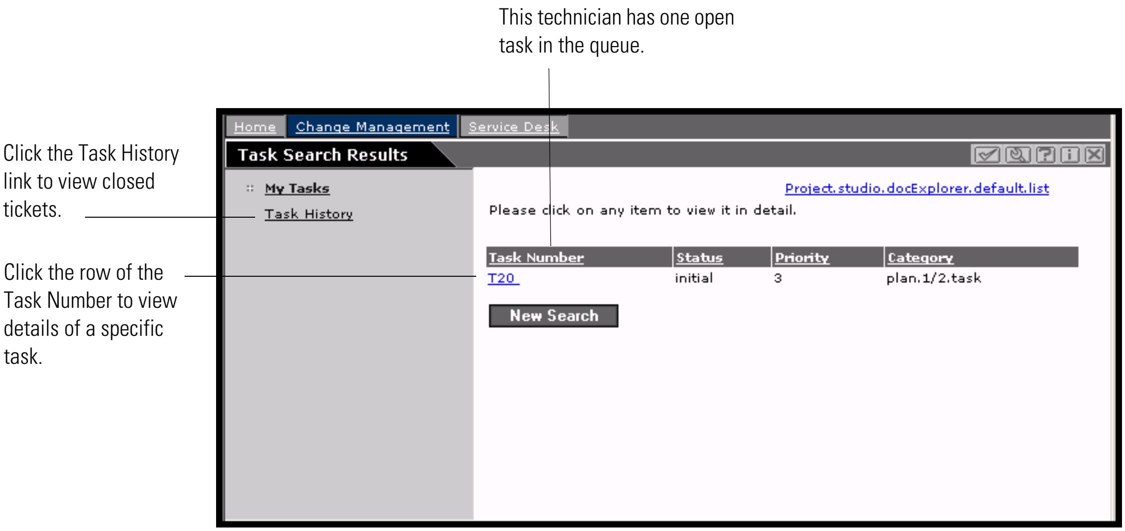
Description: 02/21/02 23:24:19 (FALCON): Tech support recently

Inventory

Affected Asset:
Asset Type:
Barcode:

Important: The Close Task feature closes the current phase of a task. If a task has multiple phases, and the current phase is not the last phase, the task continues to appear in the My Tasks list.

The Change Management activity menu provides access to the task details.



Please click on any item to view it in detail.

Task Number	Status	Priority	Category
T20	initial	3	plan.1/2.task

This technician has one open task in the queue.

Click the Task History link to view closed tickets.

Click the row of the Task Number to view details of a specific task.

Get-Services requires the following setup for the Change Management module.

Step 1 Modify out-of-box forms (see *Modifying Change Management forms* on page 85), as needed, and save as default forms.

Step 2 Verify that the Category field has the Lookup icon without the Eraser icon (see *Verifying the Category field for Get-Services* on page 90) on Incident Management Create Incidents and Service Management Create Calls forms.

Step 3 Configure the cm3tin registration screen in ServiceCenter (see *ServiceCenter event registration* on page 92) to process events synchronously.

Bookmarks

You can bookmark a Get-Services page as you bookmark any other Web page. You can also send a co-worker an HTTP link to a page—for example, a support representative may want to ask someone else to look at a particular ticket. The link is similar to the following:

http://webserver/oaa/e_service_status_whichone.jspId=PM10002

If the user is logged in to Get-Services, clicking on the link displays the designated page. If the user is not logged in, the login screen appears, and after the user logs in, the requested page opens.

Get-Services architecture overview

Get-Services interfaces with ServiceCenter. Access to the ServiceCenter database is through Get-Services adapters. The adapters establish a connection between the Peregrine OAA server and the ServiceCenter database.

ServiceCenter interface

Get-Services interfaces with Incident Management and Service Management in ServiceCenter 4.x and ServiceCenter 5.x. In addition, the Change Management module is available in ServiceCenter 5.x.

SCAdapter

Access to the ServiceCenter database is through the SCAdapter, set up during installation. User rights are established for the various tasks available in Get-Services with capability words in the user's operator record in ServiceCenter.

File attachments

When Get-Services is configured to interface with ServiceCenter, you can attach files such as spreadsheets, documents, or images to a Get-Services ticket. These attached files provide additional information to the support staff processing the ticket. Attached files are stored with the ticket on the server. See *File attachments* on page 94 for more detailed information about the file attachment feature.

3 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 Peregrine Portal interface. To use this information effectively, you should have knowledge of XML and the CSS2 specifications established by the W3C as outlined at www.w3.org.

Topics in this chapter include:

- *Deploying the Classic theme variations* on page 30
- *Changing the header graphic* on page 31
- *Modifying themes* on page 33
- *Editing the CSS files* on page 35
- *Changing the layers* on page 37
- *Changing the framesets* on page 39
- *Translating tailored modules* on page 41

Deploying the Classic theme variations

The Classic theme is the default theme used by applications built on Peregrine OAA. This is the theme you will use to create a customized theme for your enterprise.

There are five variations of the Classic theme:

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

These themes, as well as a number of other optional themes, are deployed with the application installation. However, once you have created your customized theme, it is recommended 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 theme(s) from the oaa\packages directory.

To deploy an alternate Classic design:

1 In a command prompt window, change directories to C:\oaa\packages.

2 Type:

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

Note: If you want to deploy both of the variations on the classic theme, type both of the theme names, separated by a space.

3 Press ENTER.

4 Open your Web browser and log in to the Admin module (localhost/oaa/admin.jsp).

5 Click **Settings**. On the Themes tab, change the following parameters:

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

b In the **Default stylesheet** field, change the parameter to the appropriate name for the CSS file (e.g., baja.css).

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

7 When the Control Panel is displayed, click **Reset Server**.

8 Refresh your browser to see the new theme.

Changing the header graphic

One of the easiest changes you can make is to add your corporate logo to the Peregrine Portal.

To change the header graphic:

1 Create the header graphic as needed to customize it for your enterprise.

Note: Your customized header log must be 514 pixels wide and 59 pixels high.

Peregrine Portal

2 Save your changes to the following file:

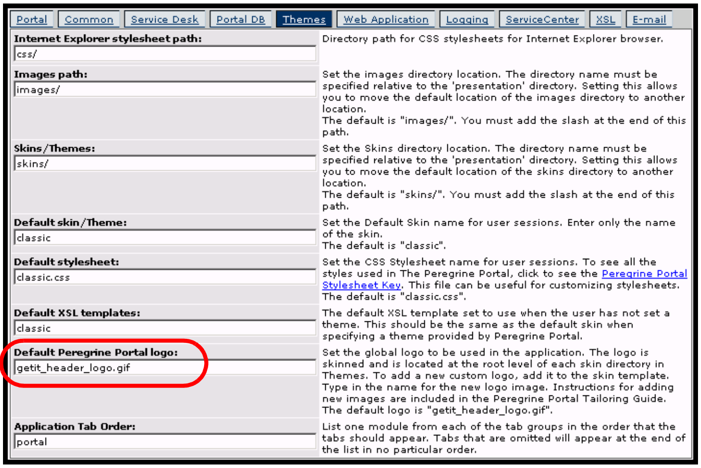
```
C:\Program Files\Peregrine\Common\Tomcat4\\webapps\oaa\images\skins\classic
```

Note: The Classic theme is the default theme.

3 Log in as an administrator (admin.jsp login page).

4 Click **Settings**.

5 On the **Themes** tab, type the new image name in the **Default Peregrine Portal logo** field.



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

Type your new image name.

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

7 When the Control Panel is displayed, click **Reset Server**.

8 Refresh the browser to view your changes.

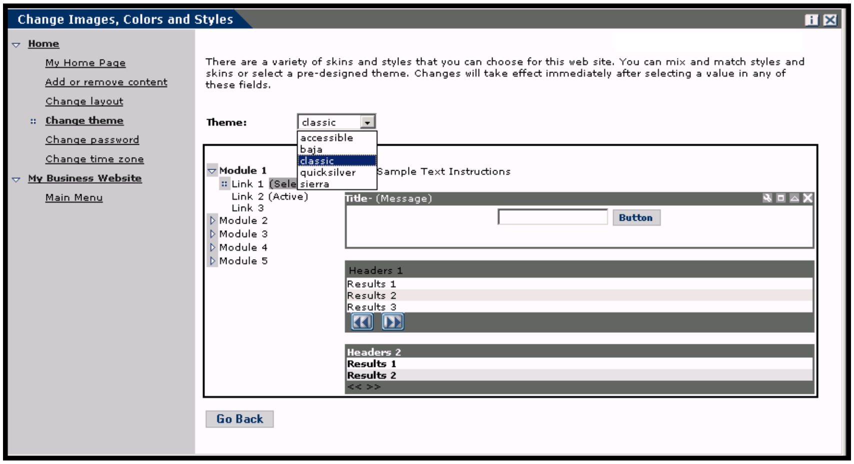
Modifying themes

For each theme folder name, there is a corresponding **css** file of the same name. For example, the classic theme has the corresponding **classic.css** file e for Internet Explorer 5.5 SP2 and 6.0, Netscape 6.x and 7.0, and Mozilla. The **css** folder is at: `C:\Program Files\Peregrine\Common\Tomcat4\webapps\oaa\css`.

To create your own theme:

1. Copy the skins\classic folder
   `C:\Program Files\Peregrine\Common\Tomcat4\webapps\oaa\css`.
2. Rename the copy of Classic to <*your corporate theme*>.
3. Edit the skin images.
   - File names must remain the same.
   - Image sizes must remain the same.

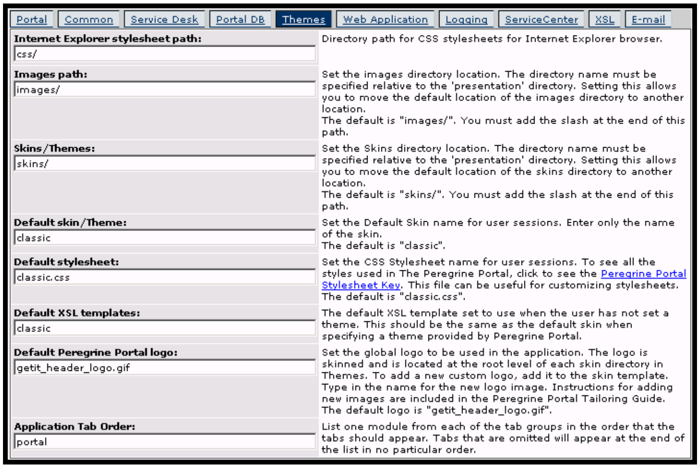
You can view the changes you made on the *Change theme* page, available from the Peregrine Portal Home page.


Change Images, Colors and Styles

There are a variety of skins and styles that you can choose for this web site. You can mix and match styles and skins or select a pre-designed theme. Changes will take effect immediately after selecting a value in any of these fields.

Theme: classic

You can also refer to the more detailed style sheet key in the themes Administration section of the Portal. To access the style sheet key, locate the Default stylesheet field on the Themes tab of the Admin Settings page and click the **Peregrine Portal Stylesheet Key** link.



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

Editing the CSS files

The following shows a portion of the **classic.css** file.

```
A,BODY,FONT,DIV,SPAN,TD,INPUT,TEXTAREA,SELECT {FONT-FAMILY: Verdana,
Tahoma, Arial, Helvetica, sans-serif;  FONT-SIZE: 10px;}
A:HOVER {COLOR; #000099;}
.ActionBar { TEXT-ALIGN: Center;}
.ActionButton {BORDER: #B5B5B5 Solid 1px; BACKGROUND-COLOR: #D6D6D6;
COLOR: #003366; CURSOR: hand; FONT-SIZE: 9px; FONT-WEIGHT: bold; }
INPUT.ActionButton:HOVER {BORDER: #B5B5B5 Solid 1px; CURSOR: hand;
BACKGROUND-COLOR: #85A5AE; FONT-SIZE: 9px;}
BUTTON.ActionButton:HOVER {BORDER: #B5B5B5 Solid 1px; CURSOR: hand;
BACKGROUND-COLOR: #85A5AE; FONT-SIZE: 9px;}
.ActionSeparator {COLOR: #1C326B;}
.ActiveHeaderMenu { BORDER-BOTTOM: #330099 Solid 1px; BORDER-RIGHT:
#330099 Solid 1px; BORDER-TOP: #330099 Solid 1px; BORDER-LEFT: #330099 Solid
1px; BACKGROUND-COLOR: #F8F8F8; COLOR: #ffffff;  }
.ActiveHeaderLink { COLOR: #ffffff;   TEXT-TRANSFORM: uppercase;}
.ActiveTabMenu {line-height: 18px; color: #FFFFFF; background-color: #666666;
padding-top: 2px; padding-right: 6px; padding-bottom: 2px; padding-left: 6px;
border-color: #CCCCCC #999999 #000000 #666666; cursor: hand; border-style:
groove; border-top-width: 1px; border-right-width: 1px; border-bottom-width: 1px;
border-left-width: 1px}
.ActiveMenuLink {COLOR: #0F2091;CURSOR: hand;  FONT-WEIGHT: Bold; }
.ActiveTableRow {COLOR: #0F2091; }
.ActiveTableNavigationRow { BACKGROUND-COLOR: #666666; COLOR: #B7C2E8;
FONT-WEIGHT: Bold; TEXT-ALIGN: Center; }
.BackgroundImage {BACKGROUND-IMAGE:
url(../images/skins/classic/backgrounds/bkg_sideframe_tile.gif);}
.Body,.BodyAlt,.BodyHead { BACKGROUND-COLOR: #ffffff; }
.BodyHeadAlt {BACKGROUND-COLOR: #D0D0D0; BACKGROUND-IMAGE:
url(../images/skins/classic/backgrounds/bkg_sideframe_tile.gif);}
.CurrentModuleMenu  { COLOR: #1A1A1A;  FONT-WEIGHT: Bold; }
A.CurrentModuleMenu:HOVER { COLOR: #000099; }
.DocTableRow {BACKGROUND-COLOR: #ffffff; COLOR: #000000;  FONT-SIZE: 10px;
BORDER-BOTTOM: #C0C0C0 Solid 2px;}
.EntryTableHeading { BORDER-BOTTOM: #e0e0e0 Solid 1px; BORDER-RIGHT:
#e0e0e0 Solid 1px; BORDER-TOP: #e0e0e0 Solid 1px; BORDER-LEFT: #e0e0e0 Solid
1px; BACKGROUND-COLOR: #09355A; COLOR: #ffffff;  FONT-WEIGHT: Bold;
TEXT-ALIGN: Left; }
```

The font family, size, weight and color, as well as other parameters such as the background color for the style are defined in this file. Some of the more commonly-modified styles are in the following table.

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.

Important: Make a copy of classic.css before you modify it. You can then create a new css file.

Modify the style sheets after you complete the overall design using the image editor's color picker to ensure that the hexadecimal choices are as true to the logo and design as possible.

Changing the layers

Layers are implemented using the *div* tag. Each div tag has an id attribute describing its function in the header. Decide which functionality you wish to retain or omit in your new header, and then modify the appropriate tags.

The following div tags are required:

- logo div
- time div
- toolbar div
- user div
- tabs div
- form titles div

Save your modifications to your deployment directory and then refresh your browser to view the changes.

The following code samples show how the div tags work. These samples are from the layers_ie.jsp file located at
C:\Program Files\Peregrine\Common\Tomcat4\webapps\oaa\images\skins\classic
and are for Internet Explorer. Corresponding files for Netscape have a _gecko or _ns designation. Make sure that you modify all files if your application is used in both Internet Explorer and Netscape browsers, and that you make the modifications in the corresponding JSP file in your corporate theme folder.

Positions the logo layer in the header:

```
<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>
```

Positions the time and alert line layer used for debugging and alerts:

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

Positions the toolbar buttons layer located currently in the upper right section of the header:

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

Positions the name of the currently logged-in user in the header:

```
<div id="user" style="position:absolute; top: -4px; right: 0px; z-index: 14;">
<table width="100%" border="0" cellpadding="0" cellspacing="0" align="right">
<tr>
<td width="50%">&nbsp;</td>
<td nowrap width="3" align="right" valign="top">
<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>&nbsp;&nbsp;</td>
</tr>
</table>
</div>
```

Positions the navigational tabs in the header:

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

Positions the page title layer in the header:

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

Changing the 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. To do so will result in JavaScript errors in your application.

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 corporate 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>
```

Translating tailored modules

Out of the box, all Peregrine OAA web applications are provided in English. You can order translated versions of the core Peregrine OAA web applications by purchasing a language pack. Peregrine OAA 4.0 language packs are available in the following languages:

- French
- Italian
- German

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

If you tailor your translated web applications, however, then you will need to translate any strings that you added. The following sections describe how you can translate your tailored modules.

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 41.

If you do not have a language pack version of your Peregrine OAA web applications and you want to create a new translation, refer to the instructions in *Adding new translation strings files* on page 43.

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 43.

Editing existing translation strings files

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

To edit an existing translation string file:

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

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

<application server install>\webapps\oaa\WEB-INF\strings

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

2 Search for any new text that you added to your tailored Get-It web application.

The string file uses the format illustrated below:

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

Where *String_label* is the Peregrine Studio name given to the string, and

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

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

```
EMPLOOKUP_EMPLOYEELOOKUP_SEARCH_LABEL, "Search"
```

3 Copy the entire line containing the English string.

4 Open the string file for the target language in which you want to add a translation.

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

5 Paste the copied English string into the target string file. You can paste the string at the end of the string file.

6 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"
```

7 Save the new string file.

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

Adding new translation strings files

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

Important: Peregrine does not support Get-It web applications translated into any languages other than those listed in *Translating tailored modules* on page 41.

To add an existing translation string file:

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

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

<application server install>\webapps\oaa\WEB-INF\strings

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

2 Copy the entire the English string file.

3 Create a new string file for the target language in which you want to add a translation.

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

4 Paste the copied English string file into the new file.

5 Change the "*translated string*" portion of each string to the target language of your translation.

6 Save the new string file.

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

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

1 Log in as an administrator (the administrator login page is located at admin.jsp).

2 Click **Settings**.

3 Click the **Common** tab.

4 Enter the two letter ISO-639 language code for the languages you want to support in the **Locales** field. The first code entered will be the default language used. The other languages you define will be available in a drop-down list.

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

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

6 Click **Save** at the bottom of the Settings form to save your changes.

7 On the Console form, click **Reset Server** to implement your changes.

Users will now be able to select the display language for their session used when they login to the Peregrine OAA Platform.

4 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-Services uses. For more advanced changes to the portal, see the chapter on *Customizing the Peregrine Systems Portal*.

Topics in this chapter include:

- *Logging in to the Peregrine Portal* on page 46
- *Using the Activity menu* on page 47
- *Personalizing the Peregrine Portal* on page 48

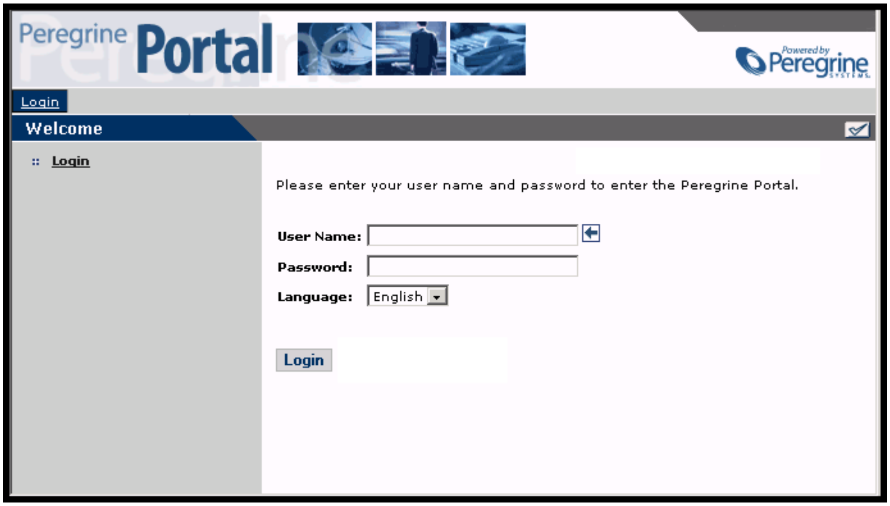
Logging in to the Peregrine Portal

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

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

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

The following is an example of the user login interface.



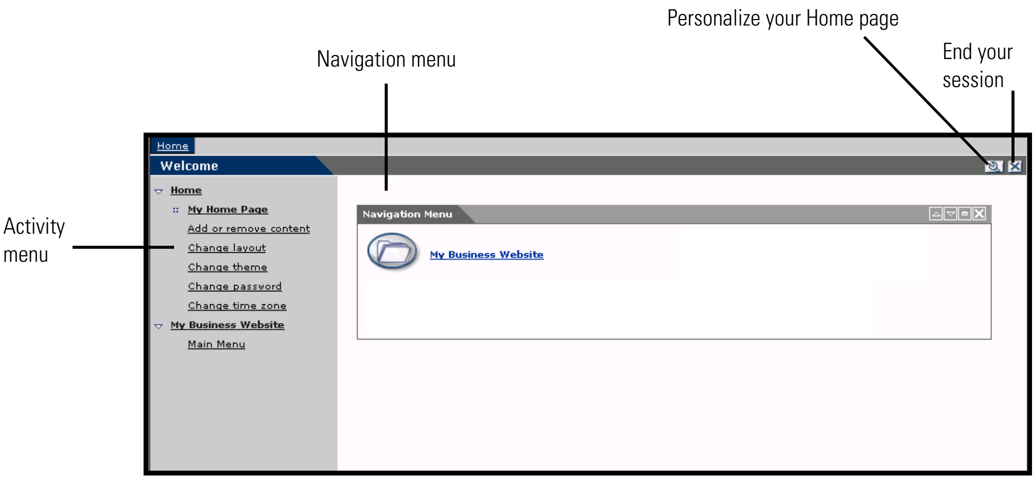
Please enter your user name and password to enter the Peregrine Portal.

User Name:

Password:

Language: English

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



Using the Activity menu

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

The default Activity menu includes the following choices:

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

Personalizing the Peregrine Portal

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

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

Adding components

The following components are available:

Personal Utilities

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

Peregrine Portal Web application components

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

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

Administration components

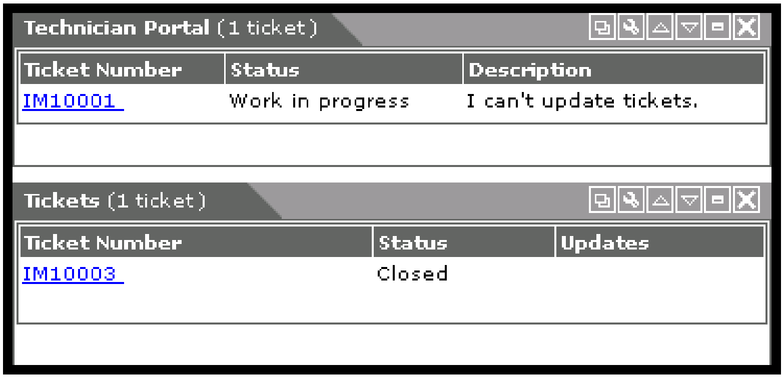
Only users with Admin capability have access to the Admin components.

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

Get-Services components

Users who have Service Management enabled can add a listing of their tickets to their Home page.

This component	Provides
Technician Portal	A display for technicians to look at their tickets.
Tickets	A list of tickets. Incidents are created when your request for service has been assigned to someone in the solution center.



Technician Portal (1 ticket)

Ticket Number	Status	Description
IM10001	Work in progress	I can't update tickets.

Tickets (1 ticket)

Ticket Number	Status	Updates
IM10003	Closed	

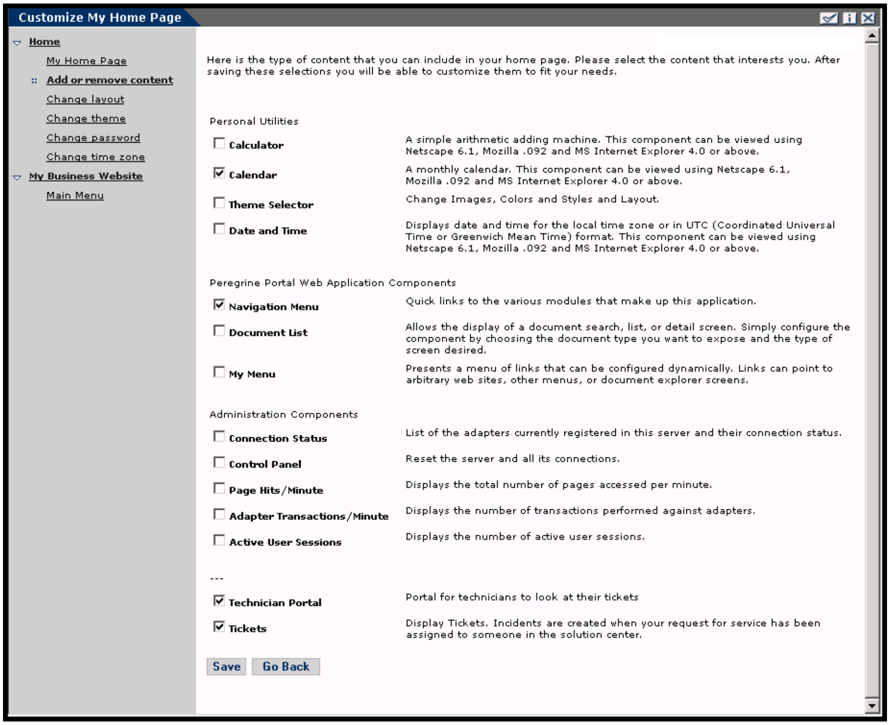
Users with Service Management enabled have the option to add Technician Portal and Tickets components to their Home page.

To add Peregrine Portal components:

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

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

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



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

Personal Utilities

☐ **Calculator**

A simple arithmetic adding machine. This component can be viewed using Netscape 6.1, Mozilla .092 and MS Internet Explorer 4.0 or above.

☑ **Calendar**

A monthly calendar. This component can be viewed using Netscape 6.1, Mozilla .092 and MS Internet Explorer 4.0 or above.

☐ **Theme Selector**

Change Images, Colors and Styles and Layout.

☐ **Date and Time**

Displays date and time for the local time zone or in UTC (Coordinated Universal Time or Greenwich Mean Time) format. This component can be viewed using Netscape 6.1, Mozilla .092 and MS Internet Explorer 4.0 or above.

Peregrine Portal Web Application Components

☑ **Navigation Menu**

Quick links to the various modules that make up this application.

☐ **Document List**

Allows the display of a document search, list, or detail screen. Simply configure the component by choosing the document type you want to expose and the type of screen desired.

☐ **My Menu**

Presents a menu of links that can be configured dynamically. Links can point to arbitrary web sites, other menus, or document explorer screens.

Administration Components

☐ **Connection Status**

List of the adapters currently registered in this server and their connection status.

☐ **Control Panel**

Reset the server and all its connections.

☐ **Page Hits/Minute**

Displays the total number of pages accessed per minute.

☐ **Adapter Transactions/Minute**

Displays the number of transactions performed against adapters.

☐ **Active User Sessions**

Displays the number of active user sessions.

☑ **Technician Portal**

Portal for technicians to look at their tickets

☑ **Tickets**

Display Tickets. Incidents are created when your request for service has been assigned to someone in the solution center.

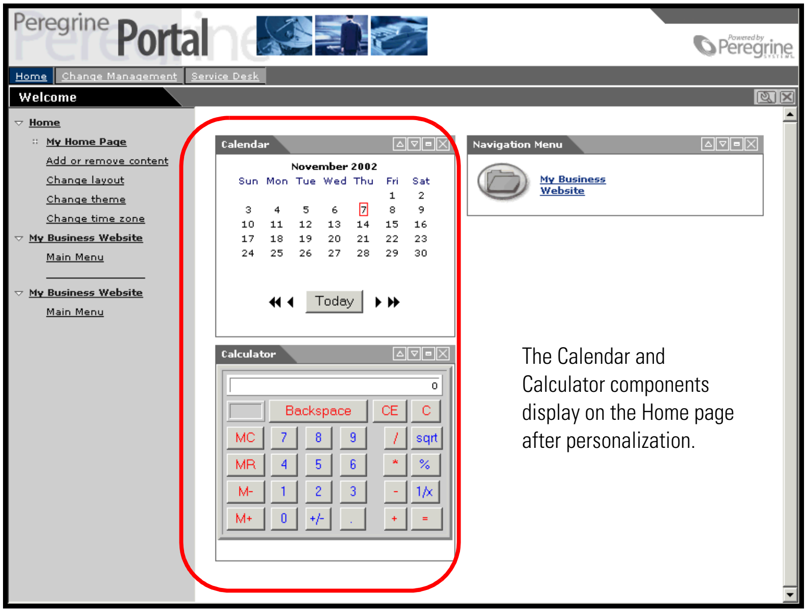
Save Go Back

Only users with Admin capability see the Administration Components.

2 Select the components you want to add to your Peregrine Portal.

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

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



November 2002

Sun	Mon	Tue	Wed	Thu	Fri	Sat
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30

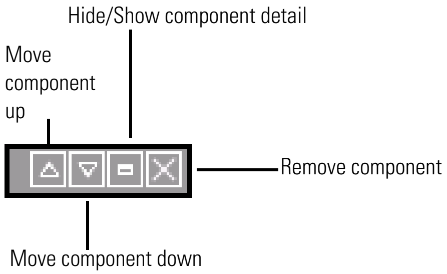
The Calendar and Calculator components display on the Home page after personalization.

Changing the layout

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

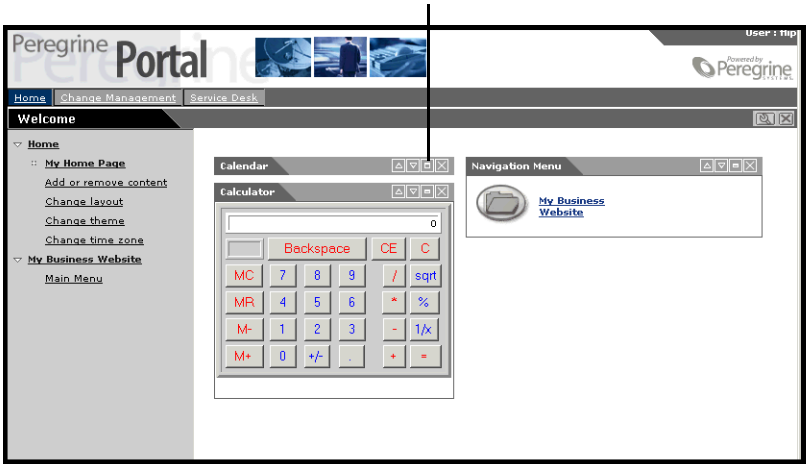
Microsoft Internet Explorer

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



In the following screen, the Calendar is minimized.

Click the Show/Hide detail button to redisplay hidden components.

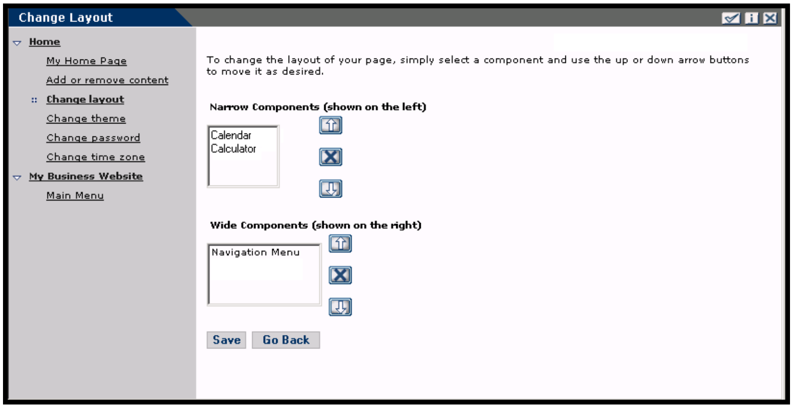


Netscape Navigator

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.



To change the layout of your page, simply select a component and use the up or down arrow buttons to move it as desired.

Narrow Components (shown on the left)

Calendar
Calculator

Wide Components (shown on the right)

Navigation Menu

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**.

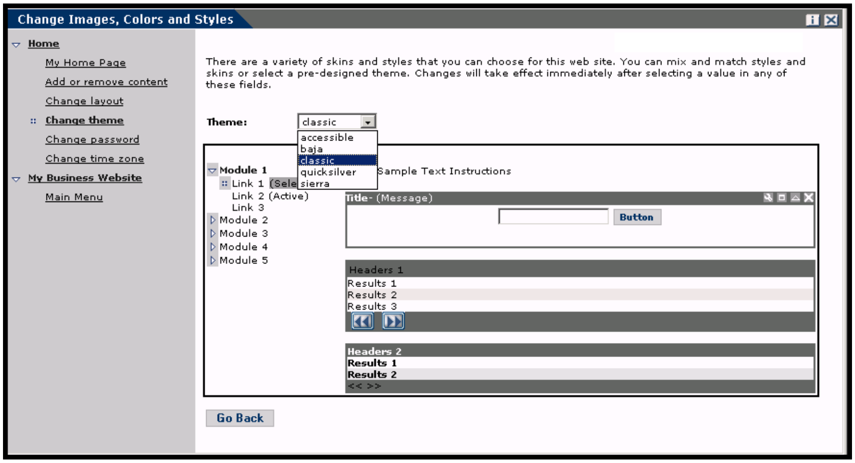
Changing themes

You can choose from a number of themes to change the look of your Web pages.

To change the theme:

1 From the Activity menu on the Portal Home page, select **Change theme**.

The following page opens.

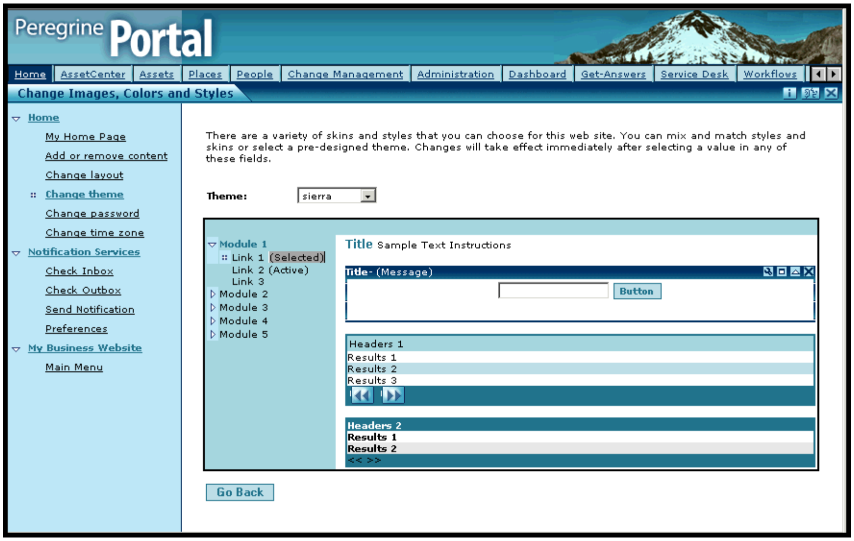


There are a variety of skins and styles that you can choose for this web site. You can mix and match styles and skins or select a pre-designed theme. Changes will take effect immediately after selecting a value in any of these fields.

Theme: classic

2 Choose from the drop-down list.

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



There are a variety of skins and styles that you can choose for this web site. You can mix and match styles and skins or select a pre-designed theme. Changes will take effect immediately after selecting a value in any of these fields.

Theme: sierra

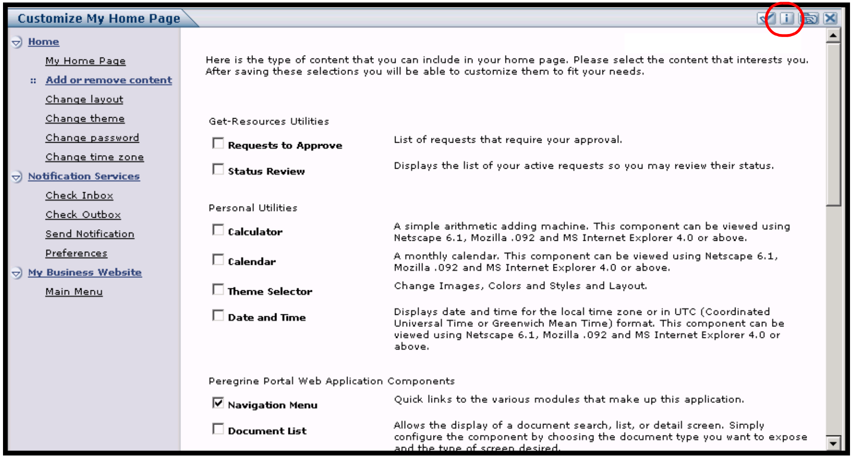
This new configuration remains through subsequent work sessions until changed.

Displaying form information

You can view information about the form you are using. Set this parameter from the Logging tab on the Settings page of the Admin module. See the Get-Services 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.



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

Get-Resources Utilities

□ **Requests to Approve** — List of requests that require your approval.

□ **Status Review** — Displays the list of your active requests so you may review their status.

Personal Utilities

□ **Calculator** — A simple arithmetic adding machine. This component can be viewed using Netscape 6.1, Mozilla .092 and MS Internet Explorer 4.0 or above.

□ **Calendar** — A monthly calendar. This component can be viewed using Netscape 6.1, Mozilla .092 and MS Internet Explorer 4.0 or above.

□ **Theme Selector** — Change Images, Colors and Styles and Layout.

□ **Date and Time** — Displays date and time for the local time zone or in UTC (Coordinated Universal Time or Greenwich Mean Time) format. This component can be viewed using Netscape 6.1, Mozilla .092 and MS Internet Explorer 4.0 or above.

Peregrine Portal Web Application Components

☑ **Navigation Menu** — Quick links to the various modules that make up this application.

□ **Document List** — Allows the display of a document search, list, or detail screen. Simply configure the component by choosing the document type you want to expose and the type of screen desired.

5 CHAPTER Using the Personalization Interface

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

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

This section includes:

- *Supporting Personalization* on page 58
- *Using the Personalization form* on page 59

Supporting Personalization

To support Personalization, you must have these components.

- An AssetCenter or ServiceCenter back-end database. Personalization requires you to store users' login rights and Personalization changes in one of these two databases.
- A user account with Personalization rights enabled. A user's login profile determines the level of Personalization rights Peregrine OAA grants a user. Users' Personalization rights determine not only what personalized components they can see and change, but also determine whether other users will see their Personalization changes. Peregrine OAA can display Personalization changes for an entire organization or specific user groups, but it can also limit the display of changes to a specific user.

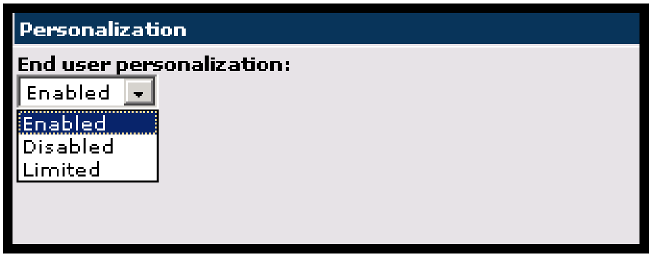
Activating Personalization

By default, Peregrine OAA defines all users as personalization end users. Peregrine OAA grants access to personalization features using the **getit.personalization** access right/capability word stored in the Web application database. See the Security chapter in this guide for more information on the available capability words. You can define the scope of end users' personalization rights by selecting one of the options from the End user personalization options on the Settings page Common tab of the Admin module.

To activate End user personalization options:

1 From the Common tab of the Admin module Settings page, scroll to the **End user personalization** parameter.

2 Select the level of personalization from the drop-down list.



Personalization

End user personalization: Enabled

You can also grant users administrator rights by adding the **getit.personalization.admin** access right/capability word to the user profile stored in the Web application database. Peregrine OAA administrator users have the following additional rights.

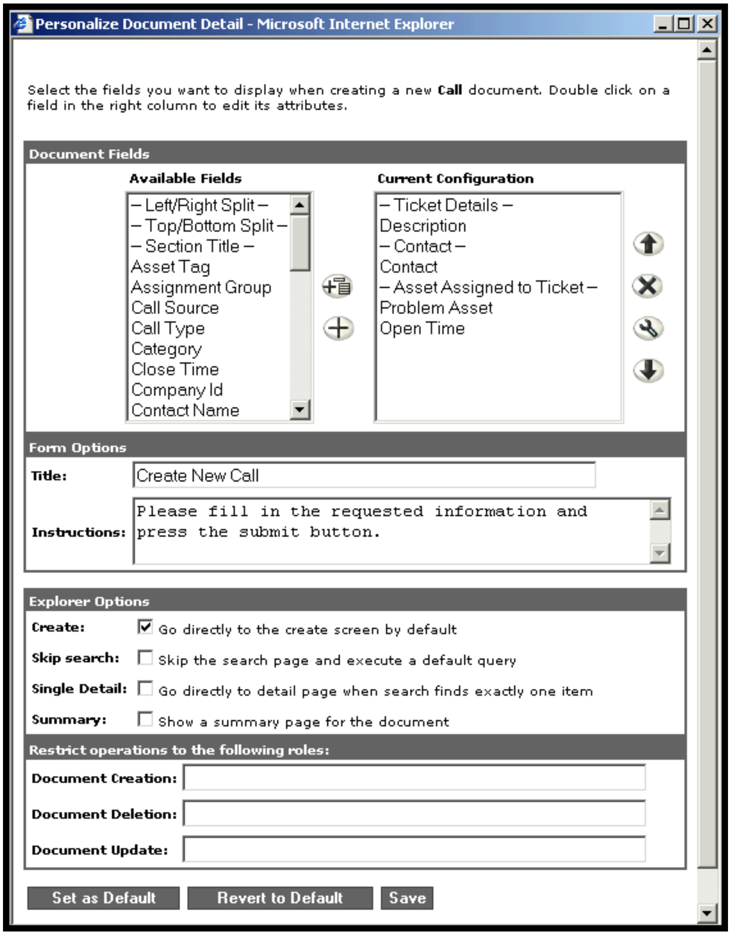
Admin capability	Description
Create	A Create button displays in search forms so that users can create new entries in the back-end database.
Update	An Update button displays in detail forms so that users can change the information that is listed for entries. Peregrine OAA also submits changes to the back-end database.
Delete	A Delete button displays in detail forms so that users can delete records from the list of entries. Peregrine OAA also deletes the record from the back-end database.
Settings are inherited by other users	This setting gives Personalization end users the proper access rights when an administrator makes Personalization changes.

Using the Personalization form

Administrators determine what available data fields display on each form. You can personalize any Web application interface that has a wrench icon in the top right of the Peregrine OAA frame. The wrench icon only appears in activities where a Personalization form has been defined. The Personalization form determines what options display in the Personalization pop-up window described below.

When you click on the Personalization icon, Peregrine OAA displays a Personalization pop-up window for the current form you are viewing.

The left column contains all the available fields of a form. The right column contains the fields that actually are on the form.



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

Document Fields

Available Fields

- – Left/Right Split –
- – Top/Bottom Split –
- – Section Title –
- Asset Tag
- Assignment Group
- Call Source
- Call Type
- Category
- Close Time
- Company Id
- Contact Name

Current Configuration

- – Ticket Details –
- Description
- – Contact –
- Contact
- – Asset Assigned to Ticket –
- Problem Asset
- Open Time

Form Options

Title: Create New Call

Instructions: Please fill in the requested information and press the submit button.

Explorer Options

Create: ☑ Go directly to the create screen by default

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

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

Summary: □ Show a summary page for the document

Restrict operations to the following roles:

Document Creation:

Document Deletion:

Document Update:

The Personalization pop-up window contains these fields:

Field	Description
Available Fields	Shows all the document fields and subdocument collections that can be added to the current form. Peregrine OAA generates the list of available fields by dynamically reading the schema that the form uses. Any items listed between dashes are form components you can use to organize and arrange how document fields are displayed in the form.
Current Configuration	Shows all the document fields, subdocument collections, and displays components that are on the current form. The first time a form is personalized, this column is empty.
Form Options Title Instructions	Defines the form name and specific instructions to follow when using the form.
Explorer Options Skip search Create Single Detail Summary	Defines how Peregrine OAA displays results. Users only see the Options section if they have sufficient 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.
Set as Default	Sets the revised configuration as the default.
Revert to Default	Removes all Personalization entered by the end user and returns the form to the default state. A default form may still display fields if the Peregrine OAA administrator or the form's schema has defined any default fields to be displayed.
Save	Saves and applies your Personalization changes to the current form.

Using the Personalize icons

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

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

Adding fields to a form

You can add fields to a form, and then change the layout.

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**.

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 *To rename labels* 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.

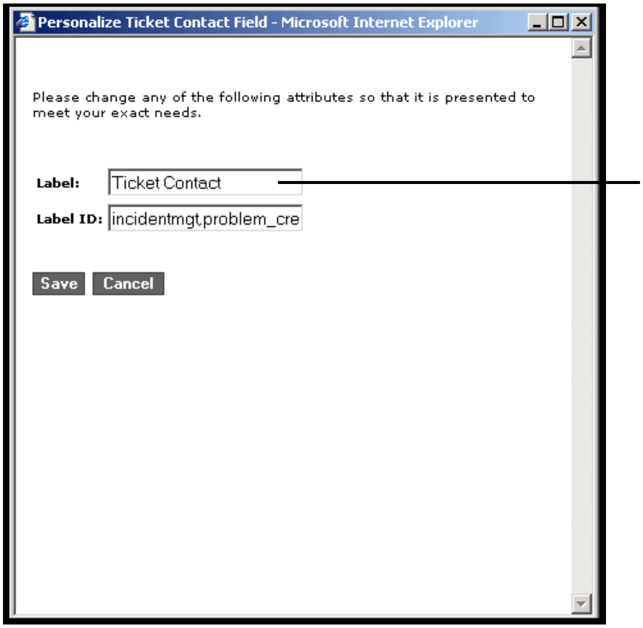
4 Click **Save** to keep your changes and return to the form.

To rename labels

1 From the Current Configuration column, select the label you want to change.

2 Click the **Personalize** (wrench) icon.

The Personalization window opens.



Personalize Ticket Contact Field - Microsoft Internet Explorer

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

Label: Ticket Contact

Label ID: incidentmgt.problem_cre

Type your changes in the text box.

3 Type the information 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.

Removing fields from the application pages

You can remove a field so that it does not display on the application pages.

To remove a field

1 From the **Current Configuration** list select a field.

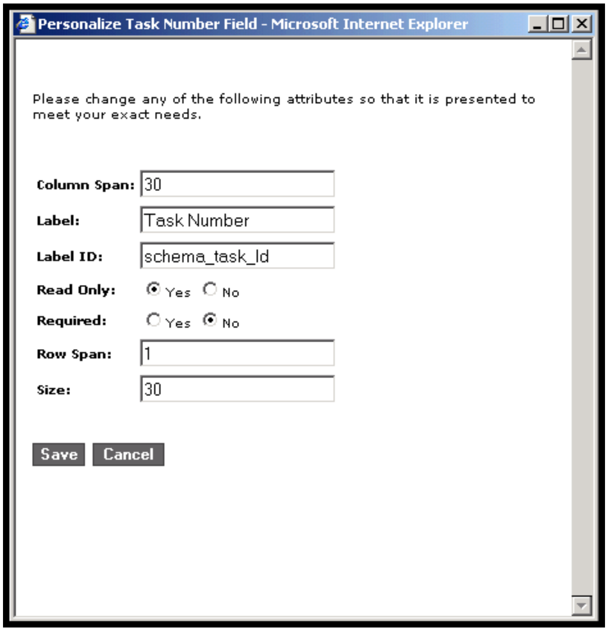
2 Click the **X** button to remove the field.

3 Click **Save**.

Configuring field attributes

To configure field attributes:

1 Double click a field from the Current Configuration list to open an edit window.



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

Column Span:	30
Label:	Task Number
Label ID:	schema_task_Id
Read Only:	● Yes ○ No
Required:	○ Yes ● No
Row Span:	1
Size:	30

2 Enter the new 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 Peregrine OAA interface.
Label ID	The schema name.
Read Only	**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.

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**.

CHAPTER 6

Get-Services Administration

This chapter includes instructions for administering your Get-Services 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-Services, you must log in as a ServiceCenter user with **getit.admin** rights to access the Admin module and administer the Get-Services integration with ServiceCenter . For a list of access capability words and Adapter configuration instructions, see the section on Get-Services security in this guide.

A default administrator, Admin, 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 `\<`*`application server`*`>\webapps\oaa\WEB-INF` directory to store these parameters. If you reinstall Get-Services, make a copy of this file and store it outside your Get-Services installation. Failure to do this will result in your parameter values being lost during the new installation.

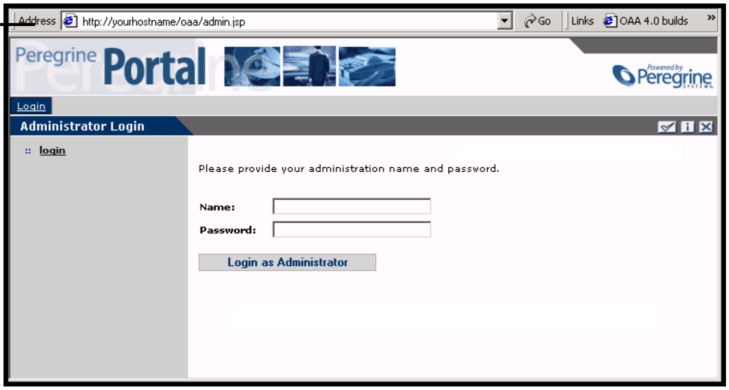
To access the Peregrine Portal administrator login page:

1. Verify that your application server (for example, Tomcat) is running.
2. In your Web browser Address field, type:

   <*hostname*>/oaa/admin.jsp

3 Press Enter to open the Portal administrator login page.

Type your hostname to connect to your local server.



Please provide your administration name and password.

Name:

Password:

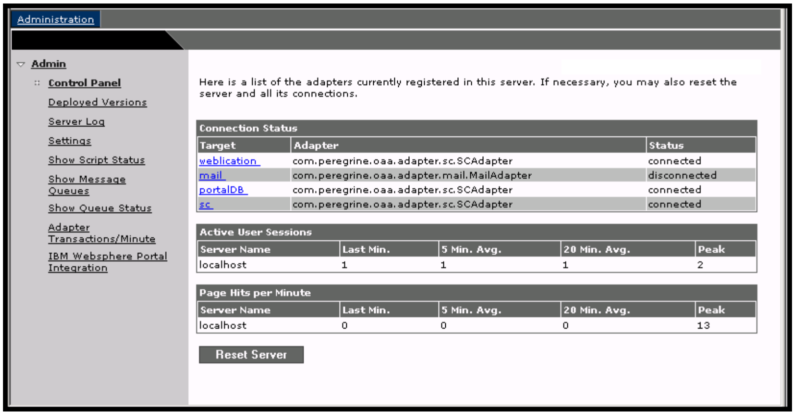
Admin is the default administrator name.

4 In the Name field, type **Admin.**

No password is required on initial login.

5 Click **Login as Administrator** to open the **Control Panel** page.

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



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

Connection Status

Target	Adapter	Status
weblication	com.peregrine.oaa.adapter.sc.SCAdapter	connected
mail	com.peregrine.oaa.adapter.mail.MailAdapter	disconnected
portalDB	com.peregrine.oaa.adapter.sc.SCAdapter	connected
sc	com.peregrine.oaa.adapter.sc.SCAdapter	connected

Active User Sessions

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

Page Hits per Minute

Server Name	Last Min.	5 Min. Avg.	20 Min. Avg.	Peak
localhost	0	0	0	13

The activities available in the Admin module include:

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

Using the Control Panel

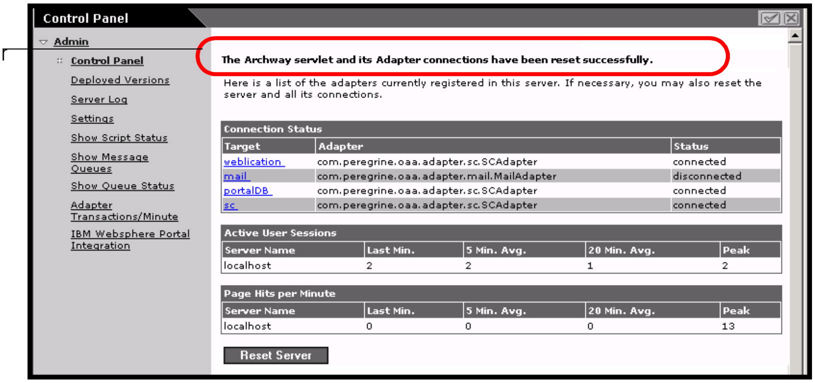
Use the Control Panel page to check the status of the connections to the databases you are accessing with Get-Services and your Web applications. You can also reset the connection between the Archway servlet and the adapters to the back-end systems.

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

▶ Click **Reset Server.**

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

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



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

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

Connection Status

Target	Adapter	Status
weblication	com.peregrine.oaa.adapter.sc.SCAdapter	connected
mail	com.peregrine.oaa.adapter.mail.MailAdapter	disconnected
portalDB	com.peregrine.oaa.adapter.sc.SCAdapter	connected
sc	com.peregrine.oaa.adapter.sc.SCAdapter	connected

Active User Sessions

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

Page Hits per Minute

Server Name	Last Min.	5 Min. Avg.	20 Min. Avg.	Peak
localhost	0	0	0	13

Viewing the Deployed Versions

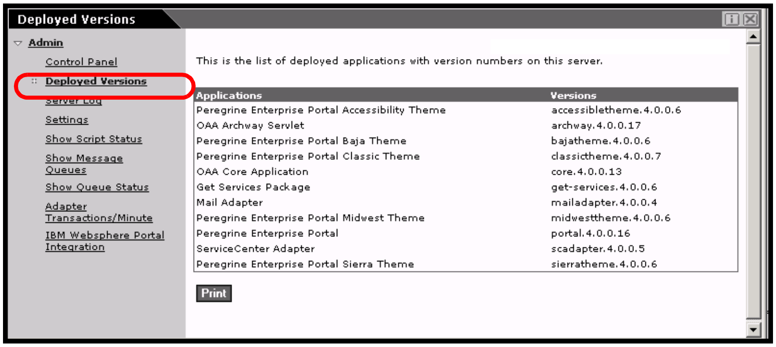
The Deployed Versions screen lists all of the packages that deploy during the installation, including the version number of each package.

To view the Deployed Versions list:

1 From the Activity menu, select **Deployed Versions.**

A list of the installed packages opens.

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



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

Applications	Versions
Peregrine Enterprise Portal Accessibility Theme	accessibletheme.4.0.0.6
OAA Archway Servlet	archway.4.0.0.17
Peregrine Enterprise Portal Baja Theme	bajatheme.4.0.0.6
Peregrine Enterprise Portal Classic Theme	classictheme.4.0.0.7
OAA Core Application	core.4.0.0.13
Get Services Package	get-services.4.0.0.6
Mail Adapter	mailadapter.4.0.0.4
Peregrine Enterprise Portal Midwest Theme	midwesttheme.4.0.0.6
Peregrine Enterprise Portal	portal.4.0.0.16
ServiceCenter Adapter	scadapter.4.0.0.5
Peregrine Enterprise Portal Sierra Theme	sierratheme.4.0.0.6

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

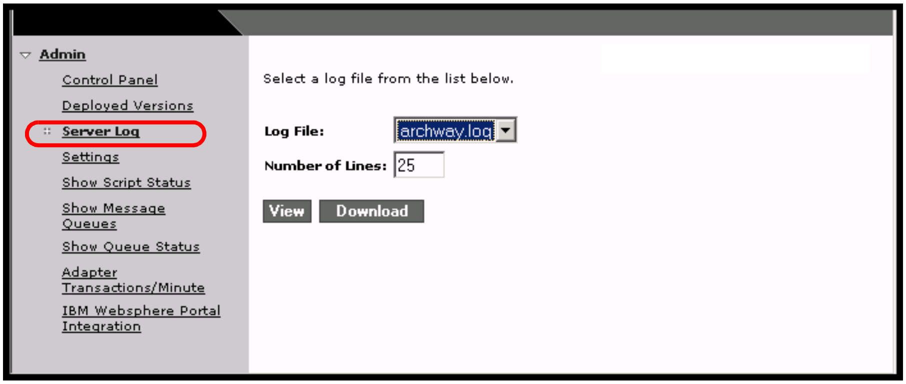
Viewing the Server Log

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

To view the Server Log:

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

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



Select a log file from the list below.

Log File: archway.log

Number of Lines: 25

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

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

3 Set the number of lines to view.

4 Do one of the following:

- Click **View** to see the log file from your Web browser.
- Click **Download** to initiate the File Download wizard that downloads the archway.log file to a location of your choice.

Using the Settings page

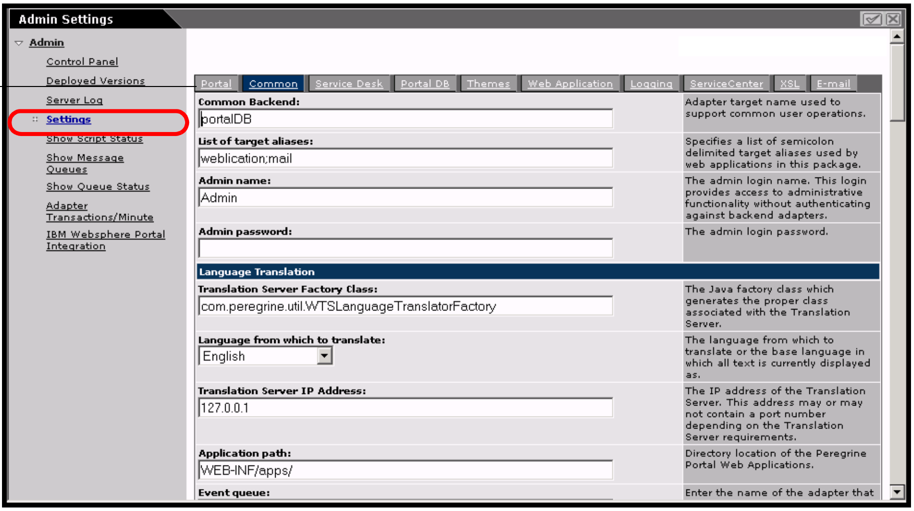
On the Activity menu, click **Settings** to open the current parameter settings. The Settings page is divided into tabs. The tabs that you see depend on the Web applications that you installed and the adapters that you use. The Common tab is available for all installations.

Settings for the Portal, PortalDB, Web Application, and Service Center (SCadapter) tabs are set during the installation (refer to the *Get-Services Installation Guide*). You can access the Settings page at any time to change the installation settings. Set the E-mail tab only when users have access to self-registration (see *User self-registration* on page 81).

To view Settings:

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

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



Common Backend: portalDB — Adapter target name used to support common user operations.

List of target aliases: weblication;mail — Specifies a list of semicolon delimited target aliases used by web applications in this package.

Admin name: Admin — The admin login name. This login provides access to administrative functionality without authenticating against backend adapters.

Admin password: — The admin login password.

Language Translation

Translation Server Factory Class: com.peregrine.util.WTSLanguageTranslatorFactory — The Java factory class which generates the proper class associated with the Translation Server.

Language from which to translate: English — The language from which to translate or the base language in which all text is currently displayed as.

Translation Server IP Address: 127.0.0.1 — The IP address of the Translation Server. This address may or may not contain a port number depending on the Translation Server requirements.

Application path: WEB-INF/apps/ — Directory location of the Peregrine Portal Web Applications.

Event queue: — Enter the name of the adapter that

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:\<*application server*>\webapps\oaa\WEB-INF directory. All changes to property settings are stored in this file. Restart Tomcat after making changes that are stored in local.xml.

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

To define a parameter:

1 Locate the setting you want to change and type the new parameter.

Note: If you have previously changed a setting and want to return to the default setting, click the **Click for default** link displayed in the description area for the parameter you want to revert. This link appears only when a setting is different from the default.

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

The Control Panel opens.

3 Click **Reset Server**.

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

Configuring Service Desk parameters

This section lists parameters that are specific to Get-Services. You configure these settings with the **Service Desk** tab on the Admin Settings page. The SCadapter, set during installation, is on the **ServiceCenter** tab (refer to the *Get-Services Installation Guide*).

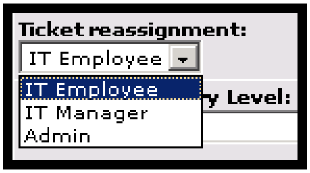
Note: The version number determines the field names for Incident Management.

Incident Management is the default module used for problem tickets opened in Get-Services with the ServiceCenter adapter. If you want end users also to create ServiceCenter call tickets, you must enable the Service Management module and configure the appropriate Get-Services settings.

To configure Get-Services settings for ServiceCenter:

1 From the Peregrine Portal Admin module, click Settings, then click the **Service Desk** tab.

2 Select an assignment group from the **Ticket reassignment** drop-down list.

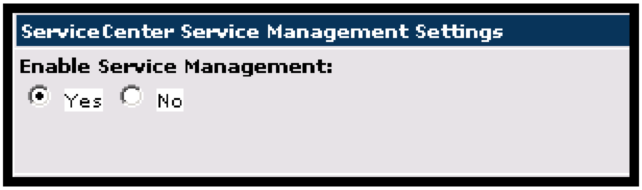


Ticket reassignment: IT Employee

User roles assigned to this field can reassign tickets to others.

3 If necessary, select **Yes** in the Enable Service Management parameter if you want tickets created from Services to be opened in the Service Management module of your ServiceCenter installation.

Note: You must have the Service Management module installed on ServiceCenter. Refer to the *ServiceCenter Administration Guide*.



ServiceCenter Service Management Settings

Enable Service Management:
● Yes ○ No

4 Scroll to the bottom of the page, then click **Save** to return to the Control Panel.

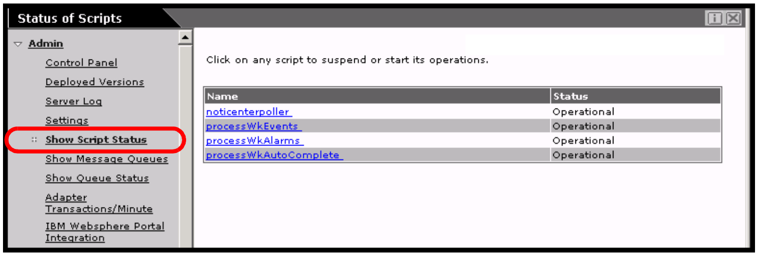
5 Click **Reset Server** to save your changes.

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.



Click on any script to suspend or start its operations.

Name	Status
noticenterpoller	Operational
processWkEvents	Operational
processWkAlarms	Operational
processWkAutoComplete	Operational

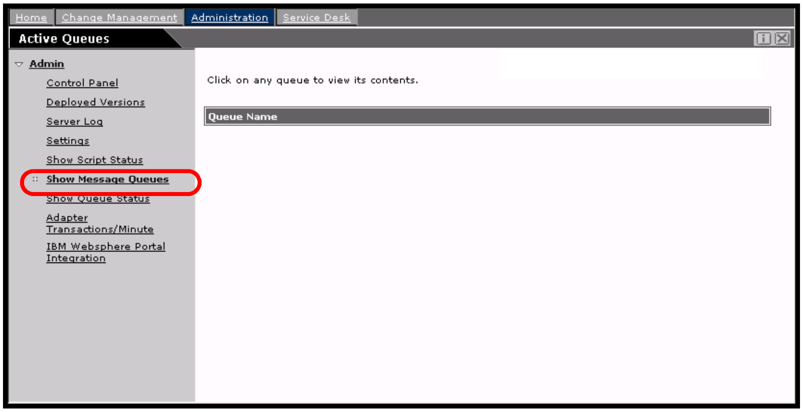
2 Click on the script to suspend it.

Displaying Message Queues

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

To display message queues:

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



Click on any queue to view its contents.

Queue Name

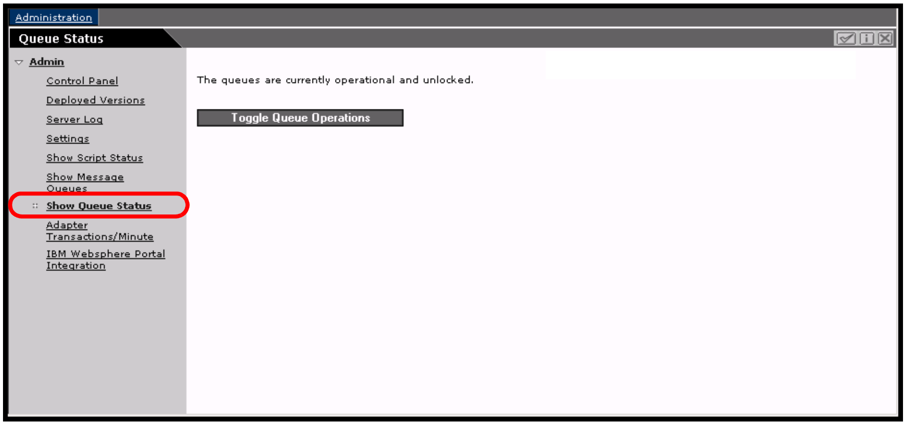
2 Click the queue name in the list to view the contents of a queue.

Showing Queue Status

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

To show queue status:

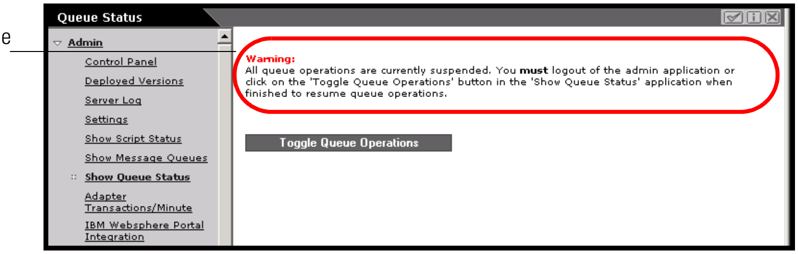
1 From the Activity menu, click **Show Queue Status** to open the Queue Status page.



The queues are currently operational and unlocked.

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

A warning message indicates that the Queue Status is suspended.



Warning:
All queue operations are currently suspended. You **must** logout of the admin application or click on the 'Toggle Queue Operations' button in the 'Show Queue Status' application when finished to resume queue operations.

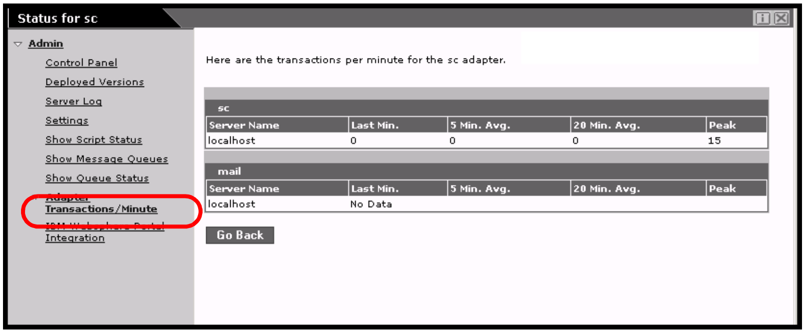
3 Click **Toggle Queue Operations** to return to the operational status.

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.



Here are the transactions per minute for the sc adapter.

sc

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

mail

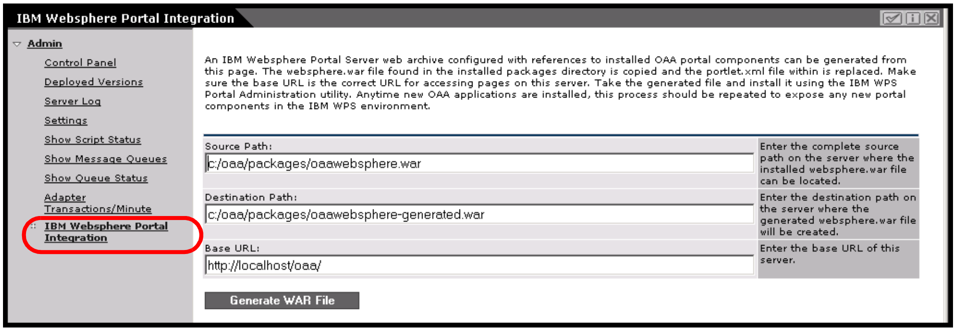
Server Name	Last Min.	5 Min. Avg.	20 Min. Avg.	Peak
localhost	No Data			

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.



An IBM Websphere Portal Server web archive configured with references to installed OAA portal components can be generated from this page. The websphere.war file found in the installed packages directory is copied and the portlet.xml file within is replaced. Make sure the base URL is the correct URL for accessing pages on this server. Take the generated file and install it using the IBM WPS Portal Administration utility. Anytime new OAA applications are installed, this process should be repeated to expose any new portal components in the IBM WPS environment.

Source Path: c:/oaa/packages/oaawebsphere.war	Enter the complete source path on the server where the installed websphere.war file can be located.
Destination Path: c:/oaa/packages/oaawebsphere-generated.war	Enter the destination path on the server where the generated websphere.war file will be created.
Base URL: http://localhost/oaa/	Enter the base URL of this server.

2 Enter the following information:

- source path
- destination path
- base URL

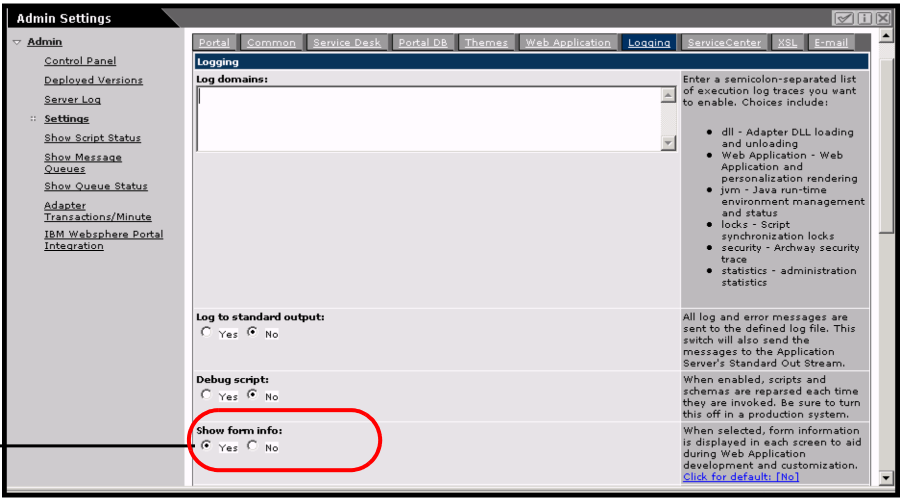
3. Click **Generate WAR File.**

Displaying form information

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

To display form information:

1. From the Admin module, click **Settings**, then **Logging**.
2. Scroll to the **Show form info** field, and click **Yes** if necessary.



Logging

Log domains:

Enter a semicolon-separated list of execution log traces you want to enable. Choices include:

- dll - Adapter DLL loading and unloading
- Web Application - Web Application and personalization rendering
- jvm - Java run-time environment management and status
- locks - Script synchronization locks
- security - Archway security trace
- statistics - administration statistics

Log to standard output: ○ Yes ● No

All log and error messages are sent to the defined log file. This switch will also send the messages to the Application Server's Standard Out Stream.

Debug script: ○ Yes ● No

When enabled, scripts and schemas are reparsed each time they are invoked. Be sure to turn this off in a production system.

Show form info: ● Yes ○ No

When selected, form information is displayed in each screen to aid during Web Application development and customization.
Click for default: [No]

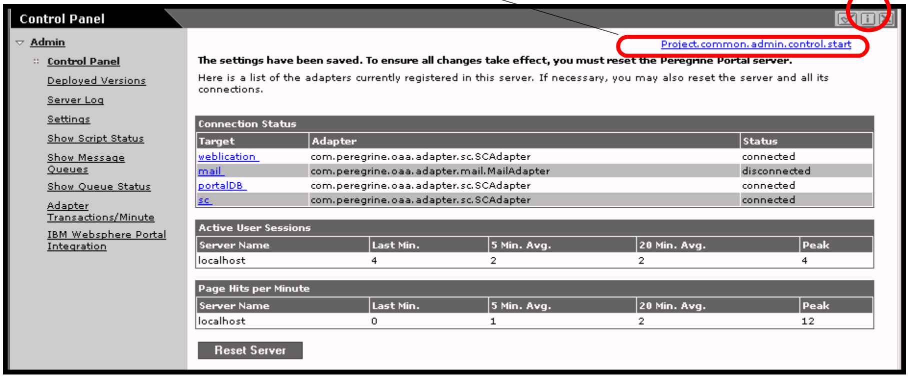
Set Show Form Info to Yes.

3. Click **Save.**

   The Control Panel opens.

4. Click **Reset Server.**

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



Project.common.admin.control.start

The settings have been saved. To ensure all changes take effect, you must reset the Peregrine Portal server.

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

Connection Status

Target	Adapter	Status
weblication	com.peregrine.oaa.adapter.sc.SCAdapter	connected
mail	com.peregrine.oaa.adapter.mail.MailAdapter	disconnected
portalDB	com.peregrine.oaa.adapter.sc.SCAdapter	connected
sc	com.peregrine.oaa.adapter.sc.SCAdapter	connected

Active User Sessions

Server Name	Last Min.	5 Min. Avg.	20 Min. Avg.	Peak
localhost	4	2	2	4

Page Hits per Minute

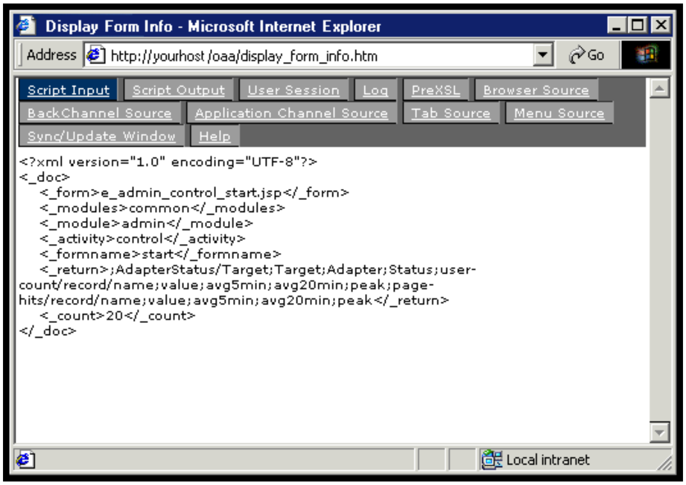
Server Name	Last Min.	5 Min. Avg.	20 Min. Avg.	Peak
localhost	0	1	2	12

The form name is at the top of the page.

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

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.



```
<?xml version="1.0" encoding="UTF-8"?>
<_doc>
   <_form>e_admin_control_start.jsp</_form>
   <_modules>common</_modules>
   <_module>admin</_module>
   <_activity>control</_activity>
   <_formname>start</_formname>
   <_return>;AdapterStatus/Target;Target;Adapter;Status;user-
count/record/name;value;avg5min;avg20min;peak;page-
hits/record/name;value;avg5min;avg20min;peak</_return>
   <_count>20</_count>
</_doc>
```

View the contents in each tab for more information 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.
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.

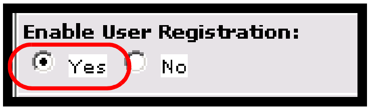
User self-registration

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 ServiceCenter database. When the user registers, ServiceCenter creates an Operator record and a Contact record for the new user with basic user login rights. See the chapter on *Security* in this guide for more information on the registration process.

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

1 From the Admin module Settings page, click **Common**.

2 Scroll to **Enable User Registration.**



Enable User Registration:

● Yes ○ No

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

3 Click **Yes.**

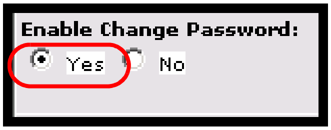
Changing passwords

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.**



Enable Change Password:

● Yes ○ No

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

3 Click **Yes.**

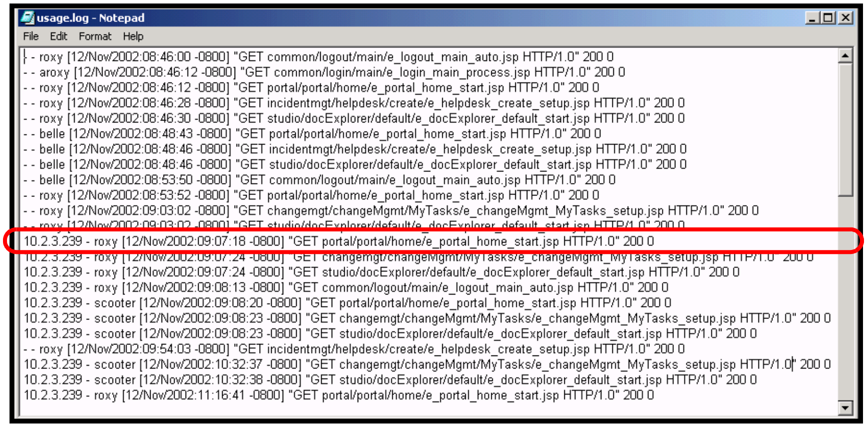
Logging and monitoring user sessions

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:

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



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

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

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

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

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

Configuring Change Management forms

You can modify Change Management out-of-box forms to use with Get-Services.

Modifying Change Management forms

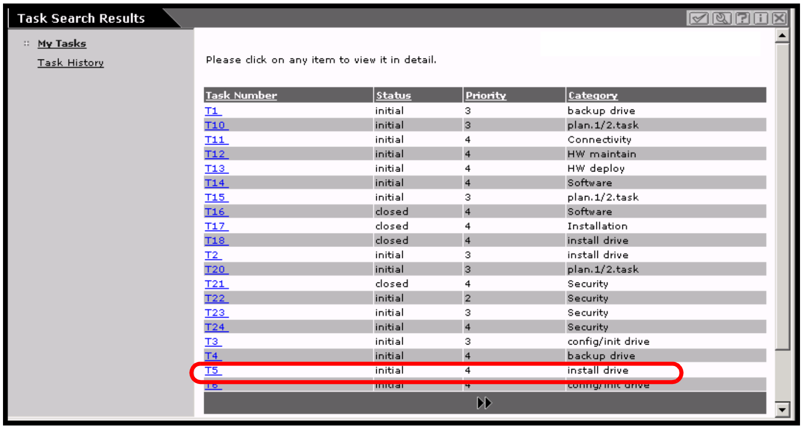
In ServiceCenter, Change and Task phases use different forms that the administrator can configure. The same functionality is available in Get-Services Change Management. Get-Services comes with the following four out-of-box forms:

Type	Phase
Change	Approval 2.plan
Task	Plan.1/2.task Security

Administrators can modify the out-of-box forms and add new forms for other categories using DocExplorer personalization (see *Using the Personalization form* on page 59). In the following example, task T5 does not have a personalized form for the Category **install drive**.

To modify forms:

1 From the Change Management tab, click **View All** to open the **Task Search Results** form.

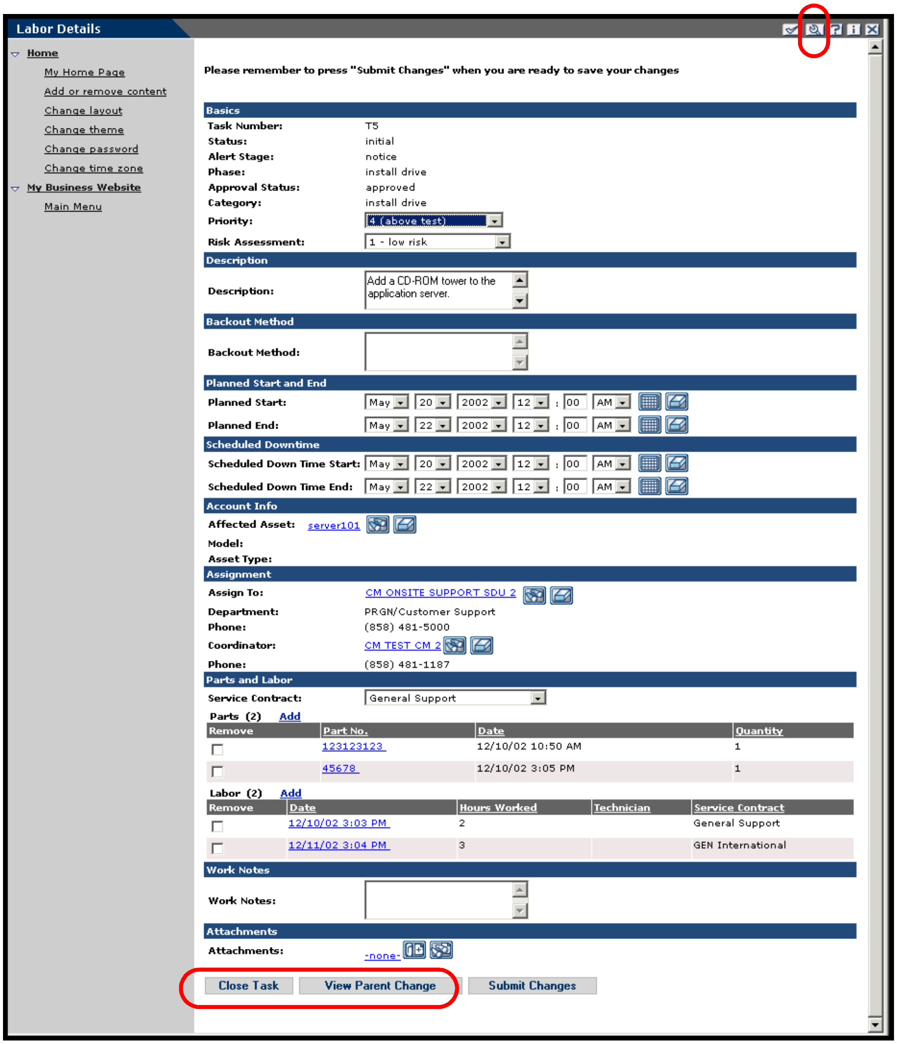


Please click on any item to view it in detail.

Task Number	Status	Priority	Category
T1	initial	3	backup drive
T10	initial	3	plan.1/2.task
T11	initial	4	Connectivity
T12	initial	4	HW maintain
T13	initial	4	HW deploy
T14	initial	4	Software
T15	initial	3	plan.1/2.task
T16	closed	4	Software
T17	closed	4	Installation
T18	closed	4	install drive
T2	initial	3	install drive
T20	initial	3	plan.1/2.task
T21	closed	4	Security
T22	initial	2	Security
T23	initial	3	Security
T24	initial	4	Security
T3	initial	3	config/init drive
T4	initial	4	backup drive
T5	initial	4	install drive
T6	initial	4	config/init drive

2 Click the row of the task you want to view to open the **Task Details** form.

Click the Modify icon to change the default form layout.



Please remember to press "Submit Changes" when you are ready to save your changes

Basics

Task Number:	T5
Status:	initial
Alert Stage:	notice
Phase:	install drive
Approval Status:	approved
Category:	install drive
Priority:	4 (above test)
Risk Assessment:	1 - low risk

Description

Description: Add a CD-ROM tower to the application server.

Backout Method

Backout Method:

Planned Start and End

Planned Start:	May 20 2002 12 : 00 AM
Planned End:	May 22 2002 12 : 00 AM

Scheduled Downtime

Scheduled Down Time Start:	May 20 2002 12 : 00 AM
Scheduled Down Time End:	May 22 2002 12 : 00 AM

Account Info

Affected Asset:	server101
Model:	
Asset Type:	

Assignment

Assign To:	CM ONSITE SUPPORT SDU 2
Department:	PRGN/Customer Support
Phone:	(858) 481-5000
Coordinator:	CM TEST CM 2
Phone:	(858) 481-1187

Parts and Labor

Service Contract: General Support

Parts (2) Add

Remove	Part No.	Date	Quantity
□	123123123	12/10/02 10:50 AM	1
□	45678	12/10/02 3:05 PM	1

Labor (2) Add

Remove	Date	Hours Worked	Technician	Service Contract
□	12/10/02 3:03 PM	2		General Support
□	12/11/02 3:04 PM	3		GEN International

Work Notes

Work Notes:

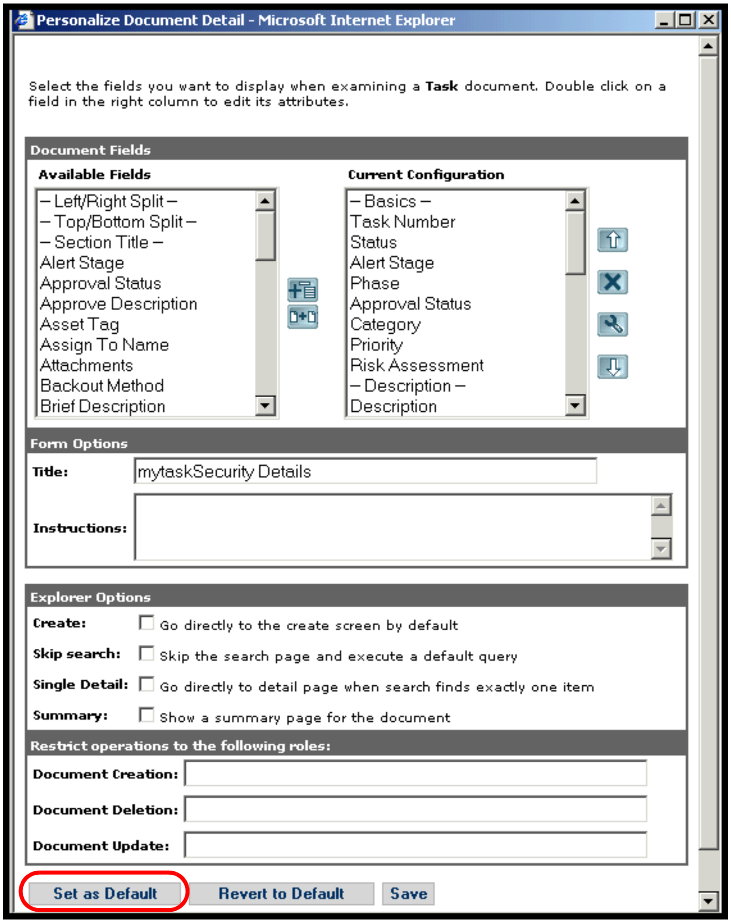
Attachments

Attachments: -none-

- Close Task is only available on the Task Details form.
- View Parent Change shows the Change details from the current task.

Warning: If Parts and Labor are not displayed in a task detail form (with personalization), updating that task may cause the existing Parts and Labor in ServiceCenter to be blanked out.

3 Click the Personalize icon to modify this personalization.



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

Document Fields

Available Fields	Current Configuration
– Left/Right Split –	– Basics –
– Top/Bottom Split –	Task Number
– Section Title –	Status
Alert Stage	Alert Stage
Approval Status	Phase
Approve Description	Approval Status
Asset Tag	Category
Assign To Name	Priority
Attachments	Risk Assessment
Backout Method	– Description –
Brief Description	Description

Form Options

Title: mytaskSecurity Details

Instructions:

Explorer Options

Create: □ Go directly to the create screen by default

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

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

Summary: □ Show a summary page for the document

Restrict operations to the following roles:

Document Creation:

Document Deletion:

Document Update:

Select Set as Default to save the form as the default.

4 Modify the form as needed, then click **Set as Default** to save it as the default form.

The saved form becomes the new default. The next time that a user accesses the Task Details of this task phase, the new personalization forms opens.

Administrators can configure forms for different categories for the following:

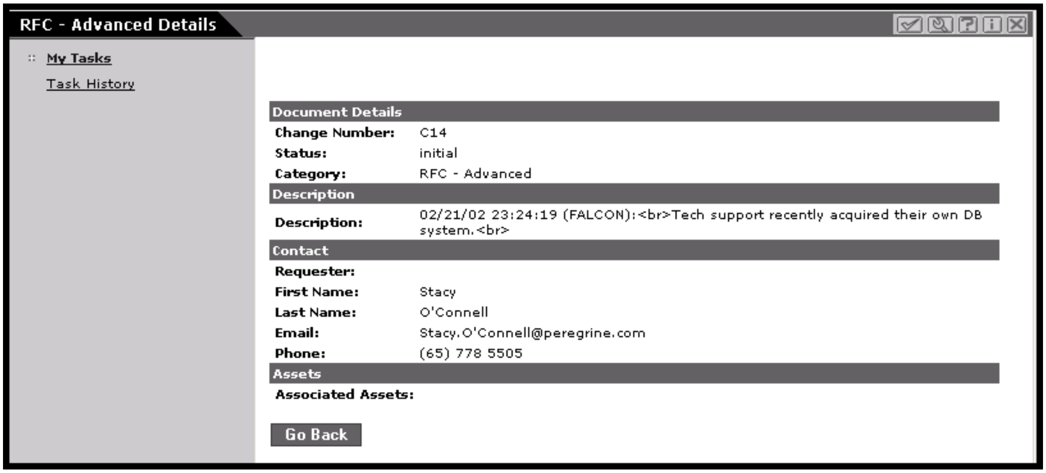
- My Task Detail forms
- Task History Detail forms
- Change Detail forms (available when users click View Parent Change from the Task Detail form)

Note: Configure the Task History Detail and Change Detail forms as Read Only (see *Configuring field attributes* on page 65 for more information on setting fields to read only).

To view the parent change details:

▶ From the **Task Details** form, click **View Parent Change**.

The Read Only **Advanced Details** form opens.



RFC - Advanced Details

Document Details

Change Number:	C14
Status:	initial
Category:	RFC - Advanced

Description

Description:	02/21/02 23:24:19 (FALCON): Tech support recently acquired their own DB system.

Contact

Requester:	
First Name:	Stacy
Last Name:	O'Connell
Email:	Stacy.O'Connell@peregrine.com
Phone:	(65) 778 5505

Assets

Associated Assets:

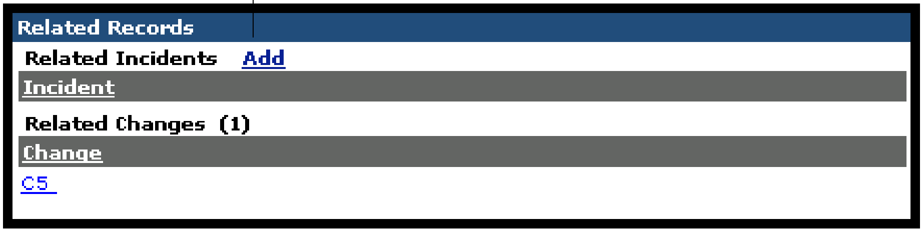
Viewing Related Records on the Details page

In Service Desk, you can view related call, incident, and change details for existing tickets in the Related Records section of the Details page. Related Incidents and Related Calls have Add capability where users can manually add tickets to the field. The Change records are read-only and do not have Add capability.

Warning: Do not personalize the Related Changes with Add capability. This field MUST remain read-only to maintain referencing integrity.

The Related Incidents field has Add capability.

The Call Details in this example has no Related Incidents and one Related Change associated with it.



Verifying the Category field for Get-Services

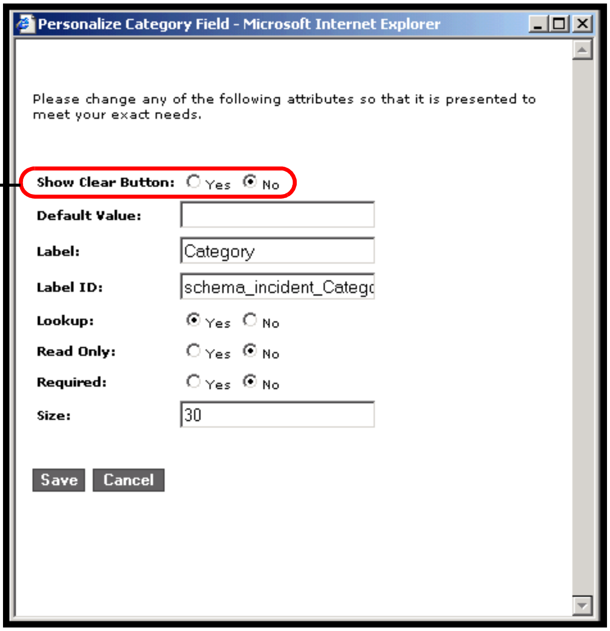
The Service Desk module has Create Incidents and Create Calls forms where technicians identify the Category using the Lookup icon. The Category field contains Subcategory, Product Type, and Problem Type fields that populate from the Lookup icon. The Eraser icon clears only one field, therefore, make sure that the Eraser icon is not on the form beside the Lookup icon.

To remove the Erase icon from the Create New forms:

1 From the Service Desk module, click **Create Incidents** to open the **Create New Ticket** form.

2 Click the Personalize icon to open the **Personalize Document Details** form.

3 From the Current Configuration column, highlight **Category** and click the Personalization (wrench) icon to open the **Personalize Category Field** form.



Personalize Category Field - Microsoft Internet Explorer

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

Show Clear Button:	○ Yes ● No
Default Value:	
Label:	Category
Label ID:	schema_incident_Catego
Lookup:	● Yes ○ No
Read Only:	○ Yes ● No
Required:	○ Yes ● No
Size:	30

Set the field to No to remove the Eraser icon in the Category field.

4 Select **No** from the **Show Clear Button** field.

5 Click **Save**, then **Set as Default.**

7 CHAPTER ServiceCenter System Administration

You must configure Get-Services to use a back-end database system. This chapter describes how ServiceCenter system administrators report Get-Services tickets and how to process events synchronously.

Topics in this chapter include:

- *Get-Services ticket reporting in ServiceCenter* on page 92
- *ServiceCenter event registration* on page 92
- *Service Management user interface changes* on page 93

Note: Incident Management is called Problem Management in ServiceCenter versions prior to 4.x. Some parameters in Incident Management use *problem* terminology because they are mapped to *problem* tables in ServiceCenter.

Get-Services ticket reporting in ServiceCenter

Get-Services enables ServiceCenter system administrators to create a report that indicates how many tickets and which tickets are opened with Get-Services. To store the Get-Services flag for tickets (problems and incidents), you must add the field `originating.system` to these tables (files):

- `probsummary`
- `problem`
- `incidents`

This procedure changes the database to support this functionality. Use this procedure once for each of the three table files, inserting the appropriate filename in the following step 2.

To change the database for Get-Services ticket reporting in ServiceCenter:

1. Log into ServiceCenter and go to Database Dictionary in the Toolkit.
2. When prompted, enter the filename for one of the three table files listed above and press Enter.
3. When the Dbdict record appears, click **New**.

   The field.window dialog box opens.
4. In the Name box, enter **originating.system**.
5. In the Type box, enter **character**.
6. Click the **plus sign** (+) to add the record.
7. Click **OK**.

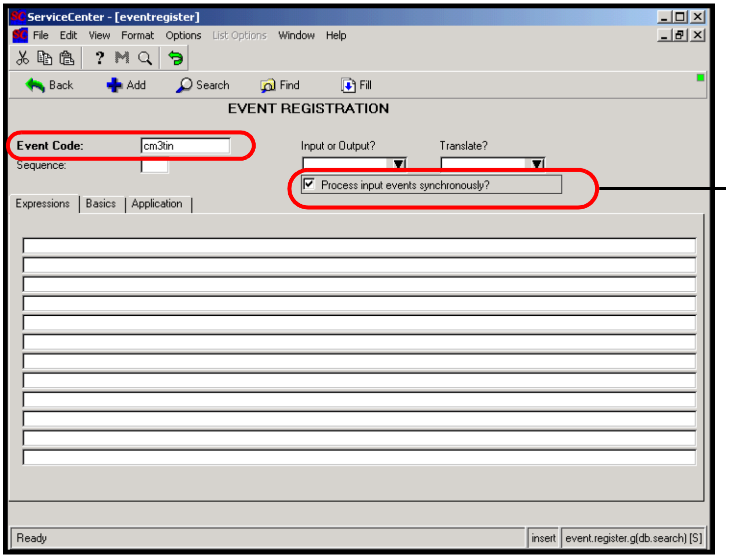
ServiceCenter event registration

The ServiceCenter administrator must make sure that **event cm3tin** is configured to process input events synchronously.

To process events synchronously:

1. From ServiceCenter, select Utilities, Event Services, Administration, Registration.

2 In the **Event Code** field, search for **cm3tin**.


ServiceCenter - [eventregister]
File Edit View Format Options List Options Window Help
Back
Add
Search
Find
Fill
Expressions
Basics
Application

EVENT REGISTRATION

Event Code: cm3tin

Sequence:

Input or Output?

Translate?

☑ Process input events synchronously?

Ready | insert | event.register.g(db.search) [S]

Verify that the field has a check.

3 Select the **Process input events synchronously?** check box, if necessary.

4 Click **Save**.

5 Re-start ServiceCenter.

Refer to the **ServiceCenter Administration Guide** for information about event registration.

Service Management user interface changes

The following interface changes occur when users access Service Management within Get-Services:

- The file attachment feature is not supported with Service Management. Therefore, the file attachment buttons and drop-down list do not appear on Call tickets. The file attachment feature only appears in Incident tickets.
- The Problem/Incident tickets and Call tickets appear as separate options on the Activity menu.
- When using the **Create Tickets** function, a Call ticket is created in ServiceCenter.

File attachments

In the Get-Services integration with ServiceCenter, users can attach files (for example, a Microsoft Excel or Word file) to Get-Services requests to provide additional information.

Attachments directory access

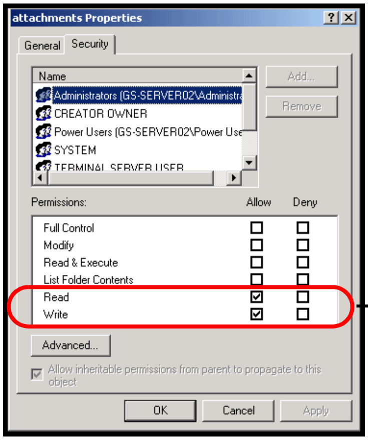
The Peregrine OAA installation creates an attachments virtual directory in the presentation directory. However, as a security safeguard to your system, use the appropriate web server administration software to change the permissions on the attachments virtual directory to only **Read** and **Write**.

The procedure below uses the Tomcat server.

To attach files:

1 Open Tomcat.

2 In the **oaa** directory, right-click on the attachments directory, and then choose **Properties**.



Name
- Administrators (GS-SERVER02\Administra
- CREATOR OWNER
- Power Users (GS-SERVER02\Power Use
- SYSTEM
- TERMINAL SERVER USER

Permissions:	Allow	Deny
Full Control	□	□
Modify	□	□
Read & Execute	□	□
List Folder Contents	□	□
Read	☑	□
Write	☑	□

☑ Allow inheritable permissions from parent to propagate to this object

Select the Read and Write permissions from the Properties dialog box.

3 Set permissions to **Read** and **Write**.

4 Click **OK.**

Attachment settings on the Common tab

The File Attachment feature uses defaults that you can override by changing the parameter in the **Common** tab of the Admin module Settings page. You can modify this parameter to set the path for the file attachments.

To set the path for file attachments:

1. From the Peregrine Portal Admin module, click Settings, then select the **Common** tab.
2. Scroll to the **Attached files' path** parameter.
3. Set the path to the directory where file attachments are saved prior to being entered in the data store.

   The default setting is `/attachments/`.

CHAPTER 8

Security

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

Password encoding methods

By default, Get-Services does not encode passwords sent over the network. Get-Services 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-Services passwords, you have three options:

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

In order to use SSL, you need to acquire a digital certificate. If your Web server has a certificate, then your Get-Services 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-Services also supports authentication via a directory service such as LDAP. When you authenticate to a directory service, Get-Services passes SHA hash encoding passwords to the service. For instructions configuring a directory service see *Custom JAAS configuration* on page 105.

Get-Services also supports Windows NT Challenge/Response 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, Windows NT Challenge/Response is only supported by Internet Explorer browsers on Windows systems. For instructions configuring Windows NT Challenge/Response see *Windows NT Challenge/Response* on page 114.

Back-end system security

This section includes information about how Get-Services authenticates users and stores personalization changes in the ServiceCenter back-end system.

Authentication with ServiceCenter

When a user logs in to Get-Services, the user name and password are validated against a corresponding **operator record** in ServiceCenter. Each operator record must contain appropriate **capability words** in order to gain access to and use different features within Get-Services.

Refer to the *ServiceCenter Administration Guide* for more information on operator records..

ServiceCenter capability words

Following is a list of available capability words for Get-Services functionality that can be assigned to an operator record in ServiceCenter:

ServiceCenter capability word	Description
getit.admin	Provides access to the OAA Admin module.
getit.change.technician	Grants access to the Change Management module of Get-Services.
getit.itemployee	Grants access to the Incident Management and Service Management modules of Get-Services. Capabilities include: updating tickets, closing tickets, viewing the list of tickets assigned, and so on.
getit.itmanager	Grants access to the Incident Management and Service Management modules of Get-Services. Users have the capabilities of itemployee in addition to assigning tickets and viewing reports.
getit.personalization.admin	Can personalize the OAA interface with admin privileges.

ServiceCenter capability word	Description
getit.personalization.default	Can personalize the OAA interface.
getit.personalization.limited	Can do limited personalization.
getit.portal	Can view the OAA home page and portal components.
getit.service	Grants basic access to Get-Services features that include opening tickets and viewing status and ticket history.
oaa.forbidden	Reserved capability word to prevent access to all OAA users.
oaa.root	Grants access to all capability words except those listed with oaa.forbidden.

Refer to the *ServiceCenter Administration Guide* for detailed instructions on assigning capability words to operator records.

ServiceCenter password security

You can set the ServiceCenter parameter **securepassword** in the ServiceCenter sc.ini file to prevent advanced users from submitting a Get-Services query that returns a list of user passwords.

To set the password security parameter in ServiceCenter:

1. Open the sc.ini file in a text editor.
2. Add the parameter **securepassword** to the file, and save the file.

   A request for a list of passwords in Get-Services returns a list with the passwords masked.

Get-Services global access rights

Although initial login access for Get-Services is validated against the user's corresponding operator record in ServiceCenter, global access rights can be granted for all users regardless of how their individual security is defined. For example, defining **getit.service** as a global access right gives all users the ability to access Get-Services even if it were not initially assigned to each user's operator record in ServiceCenter.

Global access rights are defined on the ServiceCenter settings page of the Peregrine Portal Administration module.

To define global access rights within Get-Services:

1 Open the Peregrine Portal Administration module in Get-Services.

2 In the left menu pane, click **Settings**.

- On the **Settings** pageclick the **ServiceCenter** tab.

3 In the ServiceCenter settings page, update the appropriate field with the global access right(s) that you want to grant to all users in the following format:

sc(capability word)

Multiple default access rights may be granted by separating the capability parameter values with a semicolon (;). For example:

```
sc(getit.service);sc(getit.approveritemployee)
```

Following is an example of how you would update the appropriate settings page field for ServiceCenter to grant all users the default right to access Get-Services:

Settings page	Field name	Sample field value
ServiceCenter	Default capabilities:	sc(getit.requester)

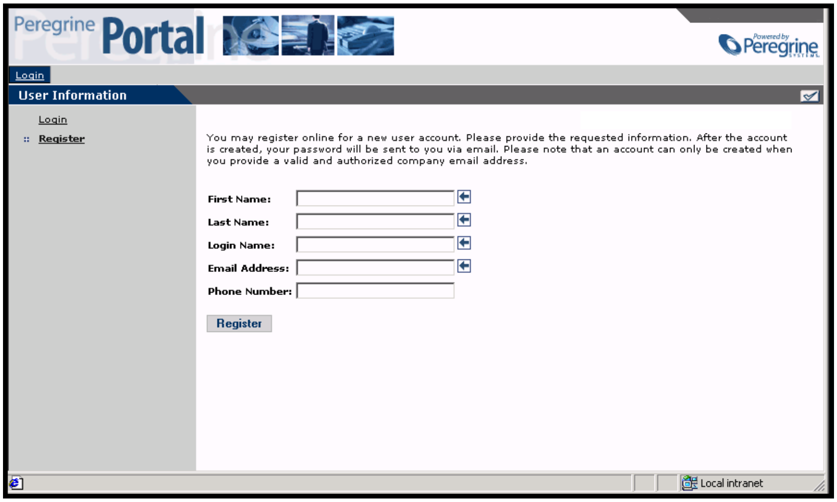
4 Scroll to the bottom of the form and click **Save**.

5 When the Control Panel page is displayed, click **Reset Server** to apply your configuration changes.

User registration

All Get-Services users need a login account in the back-end database providing authentication. For example, if you are using ServiceCenter as your back-end database, then the appropriate capability words must be defined in the user's Operator record. Similar access rights can be defined in any back-end system that you are using. The user login is automatically authenticated in the back-end system.

However, if a user is attempting to log in for the first time without back-end authentication, the user is prompted for certain default information as shown in the following screen. Note that the first four fields are required, as indicated by the arrows to the right of each field.



You may register online for a new user account. Please provide the requested information. After the account is created, your password will be sent to you via email. Please note that an account can only be created when you provide a valid and authorized company email address.

First Name:
Last Name:
Login Name:
Email Address:
Phone Number:

When the user clicks **Register**, the information is stored in the appropriate database. In ServiceCenter, Get-Services creates an operator and contact record for the new user.

Note: The appropriate back-end system adapter must be defined before the capability words are recognized. For example, if no adapter is defined for ServiceCenter, the ServiceCenter capability words are not used.

Basic registration information and login scripts are stored in the .../oaa/apps/common/jscript/ directory. Login scripts are in the login.js file. If you want to make changes to the registration process, such as changing the way a user's password is defined, you can change the scripts in this directory.

Enabling the E-mail adapter

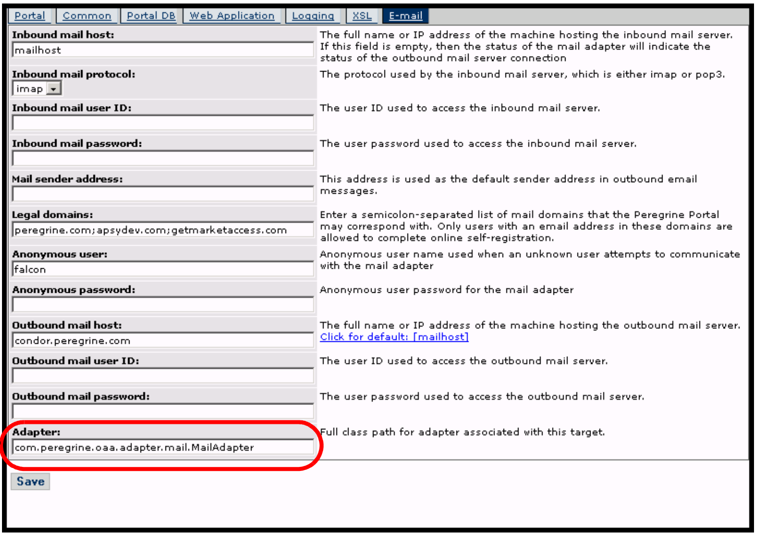
If users have the ability to self-register, you must make sure that the E-mail tab from the Get-Services Admin module Settings page contains the MailAdapter name.

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.



Inbound mail host: mailhost	The full name or IP address of the machine hosting the inbound mail server. If this field is empty, then the status of the mail adapter will indicate the status of the outbound mail server connection
Inbound mail protocol: imap	The protocol used by the inbound mail server, which is either imap or pop3.
Inbound mail user ID:	The user ID used to access the inbound mail server.
Inbound mail password:	The user password used to access the inbound mail server.
Mail sender address:	This address is used as the default sender address in outbound email messages.
Legal domains: peregrine.com;apsydev.com;getmarketaccess.com	Enter a semicolon-separated list of mail domains that the Peregrine Portal may correspond with. Only users with an email address in these domains are allowed to complete online self-registration.
Anonymous user: falcon	Anonymous user name used when an unknown user attempts to communicate with the mail adapter
Anonymous password:	Anonymous user password for the mail adapter
Outbound mail host: condor.peregrine.com	The full name or IP address of the machine hosting the outbound mail server. Click for default: [mailhost]
Outbound mail user ID:	The user ID used to access the outbound mail server.
Outbound mail password:	The user password used to access the outbound mail server.
Adapter: com.peregrine.oaa.adapter.mail.MailAdapter	Full class path for adapter associated with this target.

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 104.
- Use a custom configuration to authenticate users against user-defined adapters such as LDAP or JDBC compliant databases. See *Custom JAAS configuration* on page 105.
- 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 113.
- Use Windows NT Challenge and Response to authenticate users and pass the information to the Web application. See *Windows NT Challenge/Response* on page 114.
- Use an alternate login page and authenticate users against any of the other login options. See *Creating an alternate login page* on page 120.

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-Services 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-Services automatically generates login modules for each Peregrine adapter installed on the system.

The default login module settings are:

- loginModule=com.peregrine.OAA.security.OAALoginModule
- control flag=OPTIONAL
- options=<none>

Custom JAAS configuration

A custom JAAS configuration authenticates users against a set of JAAS LoginModules you define in a **local.xml** file. This file describes the settings to use for each JAAS LoginModule. A **local.xml** file 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.

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-Services assumes the name is a logical name to be defined in a separate adapter tag. Get-Services 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 a *required* setting for each JAAS LoginModule you use.

Use these XML tags	To do this
<controlFlag> </controlFlag>	Define what information is necessary to authenticate a user. This is a *required* setting for each JAAS LoginModule you use. See *JAAS LoginModule control flags* on page 107 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 109 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. It it succeeds, authentication does not continue to the next LoginModule in the list. If it fails, authentication continues to the next LoginModule in the list.
OPTIONAL	Authentication can proceed even if this LoginModule fails. Whether it succeeds or fails, authentication continues to the next LoginModule in the list.

Note: ControlFlag settings are case insensitive.

The overall authentication succeeds only if all Required and Requisite LoginModules succeed. If a Sufficient LoginModule is configured and succeeds, then only the Required and Requisite LoginModules prior to that Sufficient LoginModule need to have succeeded for the overall authentication to succeed. If no Required or Requisite LoginModules are configured for an application, then at least one Sufficient or Optional LoginModule must succeed.

By default, the controlFlag setting of all Get-Services Web applications LoginModules is Optional. For most enterprises, this is the desired configuration.

The following table shows some sample scenarios and how the login process works.

Module Name	Status	Scenario 1	Scenario 2	Scenario 3
LoginModule1	required	pass	pass	fail
LoginModule2	sufficient	fail	fail	fail
LoginModule3	requisite	pass	pass	pass
LoginModule4	optional	pass	fail	fail
Final Authentication		pass	pass	fail

In Scenario 1, authentication succeeds even though LoginModule2 fails. This is because the Required loginModule takes precedence over the sufficient loginModule.

In Scenario 2, authentication succeeds because the loginModules that failed are only Sufficient and Optional.

Scenario 3 authentication fails because a loginModule with a status of Required failed.

JAAS configuration options

The following tables list the possible settings for the `<options>` tag.

Standard JAAS Options

The following table lists the standard JAAS options available for all adapters.

Option	Use	Description
debug=true	optional	Instructs a LoginModule to output debugging information. The OAALoginModule logs debugging information to `stdout` and not to `archway.log`.
tryFirstPass=true	optional	The first LoginModule in the list saves the password entered and this password is used by subsequent LoginModules. If authentication fails, the LoginModules prompt for a new password and repeats the authentication process.
useFirstPass=true	optional	The first LoginModule in the list saves the password entered and this password is used by subsequent LoginModules. If authentication fails, LoginModules do not prompt for a new password.
storePass=true	optional	Stores the password for the user being authenticated.
clearPass=true	optional	Clears the password for the user being authenticated.

Peregrine JndiLoginModule options

The following table lists the options available to custom JAAS LoginModules using the Peregrine JndiLoginModule.

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.
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. **Important:** 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.

Option	Use	Description
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.
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.

Option	Use	Description
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.object Class	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 illustrates you could define a loginModule to authenticate users against an LDAP directory service.

```
<jaas_config>

  <jaasConfiguration>myconfig</jaasConfiguration>
    <myConfig>ldap</myConfig>

  <ldap>
    <loginModule>
    com.sun.security.auth.module.JndiLoginModule
    </loginModule>
    <controlFlag>REQUIRED</controlFlag>
    <options>
    user.provider.url="ldap://server/dc=peregrine,dc=com";
    group.provider.url="ldap://server/dc=peregrine,dc=com"
    </options>
  </ldap>

</jaas_config>
```

Standard Sun Microsystems JAAS configuration

The standard JAAS configuration authenticates users against the Sun Microsytems JAAS configuration loginModule. 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.

Windows NT Challenge/Response

Windows NT Challenge/Response is one of the ways Windows NT 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.

The Get-Services uses Windows NT Challenge/Response as follows:

- The user logs in to a Windows XP/2000/NT workstation.
- The user starts the IE browser and navigates to the `login.asp` page.
- IE automatically sends user authentication information to IIS. The user’s password is not transferred, but the Windows NT Challenge/Response 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 Windows NT Challenge/Response/IIS server data.
- The user is logged in without requiring that a name and password be entered.

During this process, Archway authenticates and impersonates the NT user with each of its adapters.

The following circumstances are exceptions to the normal Windows NT Challenge/Response login process:

- The Windows NT user has already registered with an Archway adapter. When this occurs, the web application asks the user to register and enter profile information. The application then lets the user log in and stores this information for future login attempts.
- The Windows NT user name is already registered as an Administrator in the back-end system. When this occurs, the web application does not proceed with automatic login. The user is presented with another login screen and is asked to verify their password. This step is an added security measure to prevent a user from accidentally logging in with administrative rights.

Setting up Windows NT Challenge/Response

Setting up Get-Services to use Windows NT Challenge/Response is a five step process:

Step 1 Set Web server properties for the login.asp file. See *Setting Web server properties for the login.asp file* on page 116.

Step 2 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 117.

Step 3 Set Web server properties for the loginverify.asp file. See *Setting Web server properties for the loginverify.asp file* on page 118.

Step 4 Define the **LogoutURL** from the Get-Services administration page. See *Setting up the LogoutURL* on page 118.

Step 5 Set permissions on the Get-Services presentation folder. See *Setting permissions for the presentation folder* on page 119.

The following procedures illustrate how to setup Windows NT Challenge/Response authentication using Windows NT as an example. If you are using Windows XP or 2000, the overall procedure is the same. However, in Windows XP and 2000, Challenge/Response is called Integrated Windows Authentication, and the IIS Management Console is called Internet Information Services.

Setting Web server properties for the login.asp file

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

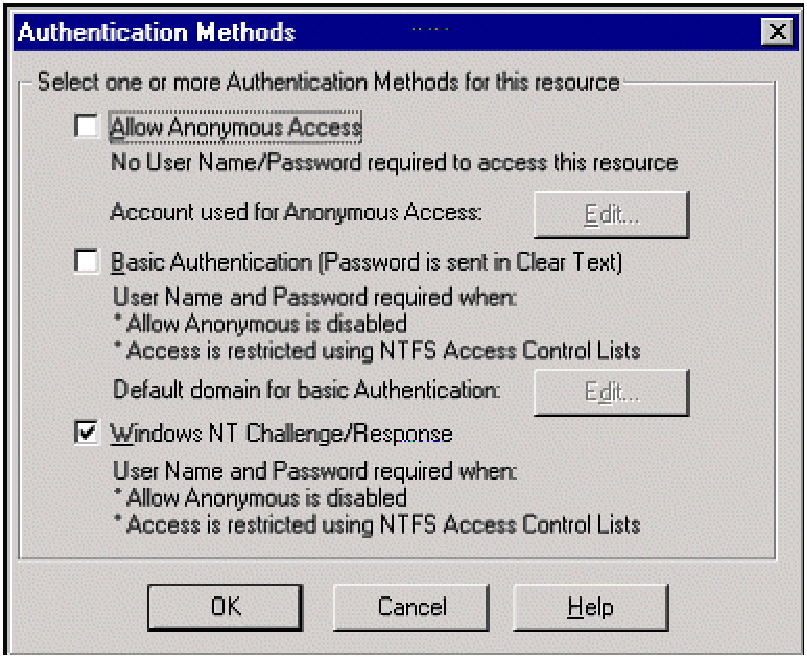
In Windows 2000 and XP, open Internet Information Services (Start>Programs>Administrative Tools>Internet Information Services)

2 Click on the oaa virtual directory.

3 Right-click on login.asp and select **Properties.**

4 Select the **File Security** tab.

5 Click **Edit** in the “Anonymous Access and Authentication Control” section.



Select one or more Authentication Methods for this resource

□ Allow Anonymous Access

No User Name/Password required to access this resource

Account used for Anonymous Access:

□ Basic Authentication (Password is sent in Clear Text)

User Name and Password required when:
* Allow Anonymous is disabled
* Access is restricted using NTFS Access Control Lists

Default domain for basic Authentication:

☑ Windows NT Challenge/Response

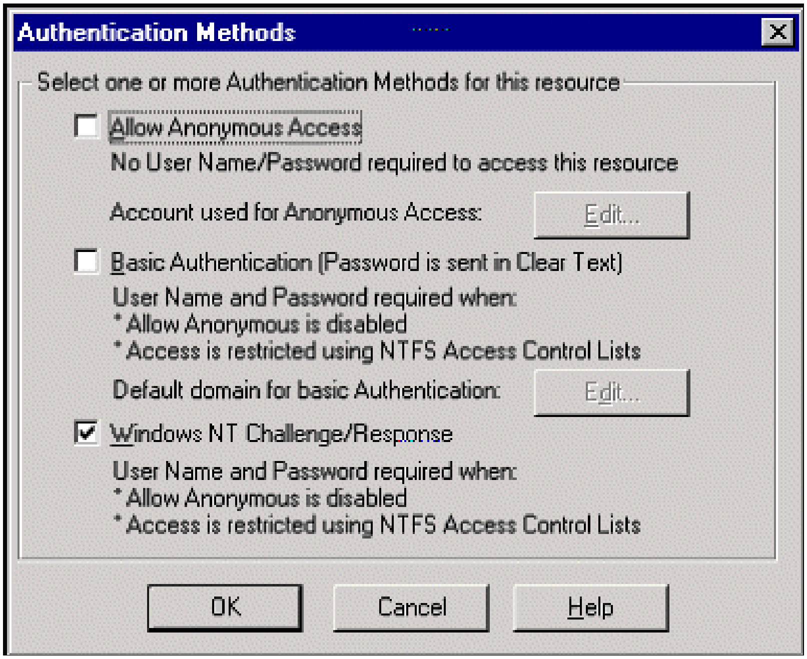
User Name and Password required when:
* Allow Anonymous is disabled
* Access is restricted using NTFS Access Control Lists

6 Check **Windows NT Challenge/Response.** Make sure this is the only option checked.

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

Setting Web server properties for the e_login_main_start.asp file

1. From the IIS Management Console, right-click on e_login_main_start.asp and select **Properties**.
2. Select the **File Security** tab.
3. Click **Edit** in the “Anonymous Access and Authentication Control” section.



Authentication Methods

Select one or more Authentication Methods for this resource

☐ Allow Anonymous Access

No User Name/Password required to access this resource

Account used for Anonymous Access: Edit...

☐ Basic Authentication (Password is sent in Clear Text)

User Name and Password required when:
* Allow Anonymous is disabled
* Access is restricted using NTFS Access Control Lists

Default domain for basic Authentication: Edit...

☑ Windows NT Challenge/Response

User Name and Password required when:
* Allow Anonymous is disabled
* Access is restricted using NTFS Access Control Lists

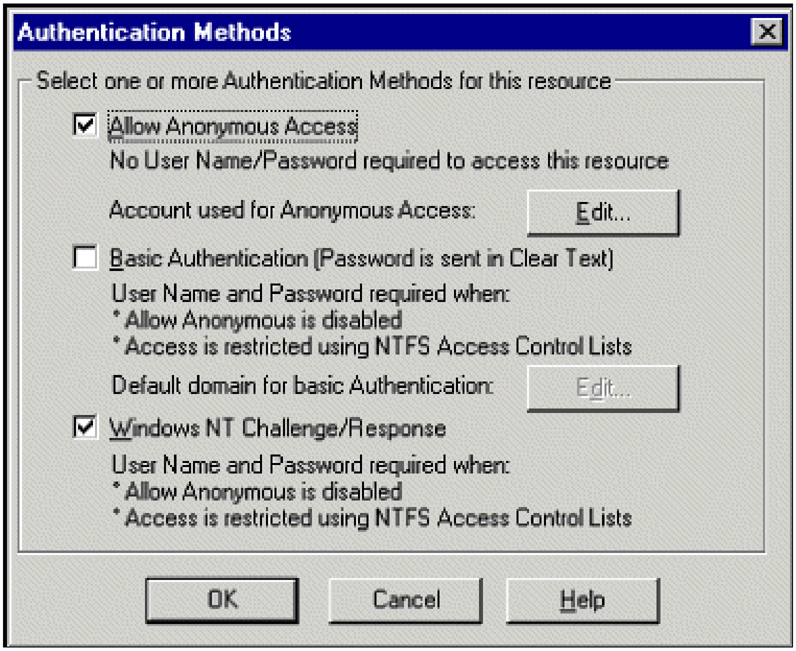
4. Check **Windows NT Challenge/Response.** Make sure this is the only option checked.
5. Click **OK** on all windows displayed until you return to the Microsoft Management Console.

Setting Web server properties for the loginverify.asp file

1 From the IIS Management Console, right-click on loginverify.asp and select **Properties**.

2 Select the **File Security** tab.

3 Click **Edit** in the “Anonymous Access and Authentication Control” section.



Authentication Methods

Select one or more Authentication Methods for this resource

☑ Allow Anonymous Access

No User Name/Password required to access this resource

Account used for Anonymous Access: Edit...

□ Basic Authentication (Password is sent in Clear Text)

User Name and Password required when:
* Allow Anonymous is disabled
* Access is restricted using NTFS Access Control Lists

Default domain for basic Authentication: Edit...

☑ Windows NT Challenge/Response

User Name and Password required when:
* Allow Anonymous is disabled
* Access is restricted using NTFS Access Control Lists

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

5 Close the Management Console.

Setting up the LogoutURL

1 Open a Web browser.

2 Enter the following URL: http://webserver/oaa/admin.asp in the browser address field (where webserver is the name of your Web server and oaa is the name of the virtual directory created during installation).

3 Login using the administrator name and password.

4 Click **Settings**.

5 From the **Common** tab, set the **LogoutURL** setting to the URL you want users to go to if Windows NT Authentication fails or is not possible due to the user's current browser.

Setting permissions for the presentation folder

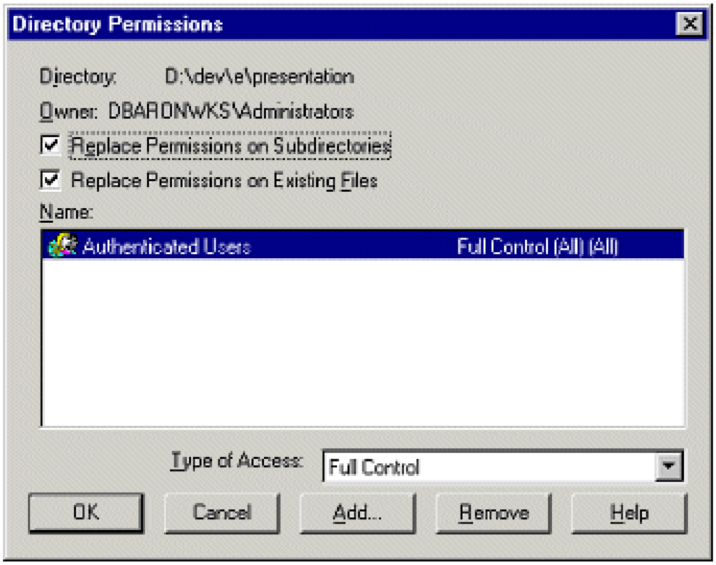
1 Use Windows NT Explorer to navigate to the ...oaa\presentation folder.

2 Right-click on presentation and select **Properties**.

3 On the **Security** tab, click **Permissions**.

Note: If you do not see a Security tab, verify that your Web application is installed on an NTFS partition.

4 Click **Add** to change the user groups that have permission to access the folder. Change the permission to a named authenticated group. For example, you could change permissions to all "Authenticated Users".



Directory Permissions

Directory: D:\dev\e\presentation

Owner: DBARONWKS\Administrators

☑ Replace Permissions on Subdirectories

☑ Replace Permissions on Existing Files

Name:

Authenticated Users Full Control (All) (All)

Type of Access: Full Control

5 If the user group called "Everyone" has permissions, highlight the entry, and then click **Remove** so that only the group you selected in the previous step can access the ProductCoreAbbreviated.

6 Click **OK**. Close all remaining windows.

Testing the settings

Log in to your Peregrine Web application to make sure the access permissions are set correctly. The Windows NT Challenge/Response settings are activated when you log in through a special login page named login.asp. Accessing your applications through the standard login.jsp page results in the users needing to log on as usual.

To test the settings:

1. Open a Web browser.
2. Enter the following URL: http://webserver/oaa/login.asp in the browser address field (where webserver is the name of your Web server and oaa is the name of the virtual directory created during installation).
3. Verify that access to Get-Services is what you expected based on the settings you chose for the login.asp and loginverify.asp files.

Creating an alternate login page

If you do not want to use the default Peregrine OAA login page, you can create your own login page that authenticates users and redirects them to the proper start page. Creating an alternate login page requires two basic steps:

Step 1 Create a login Web page with the necessary authentication parameters. See the following section, *Creating a login Web page*.

Step 2 Edit the archway.xml to specify the HTTP authentication method you want to use. See *Specifying an alternate authentication method* on page 122.

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.html is in the OAA deployment folder of your application server:

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

Customize this sample HTML form using the following guidelines:

- Whatever custom login file you create becomes part of your login URL. For example, if you create a custom page called my_login.htm, then the login URL is http://<server>:<port>/oaa/my_login.htm
- You must specify the basicauth servlet in the form action. For example, action="http://<server>:<port>/oaa/servlet/basicauth"
- Users who have the *getit.portal* capability word see the e_portal_home_start.jsp home page if successfully authenticated
- Users who do *not* have the *getit.portal* capability word see the e_home_main_start.jsp home page if successfully authenticated
- Users who fail to be successfully authenticated see the page specified in the _failURL value
- The basicauth servlet does not encrypt usernames and passwords during login. You must enable HTTPS if you are concerned about password security on your intranet.
- If no URL is specified in the form action, then authenticated users are redirected to http://<server>:<port>/oaa/login.jsp where they see either e_portal_home_start.jsp or e_home_main_start.jsp depending on their login capability words.
- There are no specific Administration page settings needed to set up a custom login page. You must define all login parameters in your custom login page.
- If you want to display a specific OAA page at login, you can specify the page in the form action URL. For example, the value action="http://<server>:<port>/oaa/servlet/basicauth/e_home_main_start.jsp" displays the non-portal version of the Peregrine OAA home 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 archway.xml file.

To specify an alternate HTTP authentication method:

1. Stop your application server.
2. Using a text editor, open the archway.xml file located at:

   <application server>\webapps\oaa\WEB-INF\default.
3. Edit the line containing:

   ```
   <httpauthclass ...>HttpBasicAuthenticationManager</httpauthclass>
   ```
4. Change the value HttpBasicAuthenticationManager to HttpAlternateAuthenticationManager.
5. Save the file.
6. 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.

Glossary

Call—a request for service or information. In ServiceCenter, a call is a means of establishing a line of communication with the service desk. A call report or incident ticket can be generated from a call to the help desk.

Category—a classification of a group of calls or incidents. ServiceCenter includes a series of default categories and administrators can create new categories. You can specify default categories for Get-Services calls and incidents in the Get-Services tab of the Peregrine Portal Admin Module.

Contact—the person who reports a problem or requests information. A contact can be an internal customer (company employee) or an external customer (a person outside the company).

Form—a ServiceCenter screen layout (or window) used to access, add, change, and view records in a specific file, or used as part of the user interaction in an application.

Help desk case—See *call*.

Help desk operator—the person who tracks and resolves problems. In ServiceCenter, this person is also known as an operator or a coordinator.

Incident—any event that requires management beyond the standard operation of the help desk and which causes or may cause an interruption to or reduction in the quality of service.

In ServiceCenter, incidents typically require resolution actions, unlike calls. The difference between a call and an incident is the level of support required for the resolution. This may be based upon the complexity of the issue, number of individuals involved, or amount of work required.

Note: Incident and problem are terms that are used interchangeably in the Get-Services interface. Incident Management is called Problem Management in ServiceCenter versions prior to 4.x. Some parameters in Incident Management use *problem* terminology because they are mapped to *problem* tables in ServiceCenter when you use the SCAdapter.

Problem—see *Incident*.

Problem Type — a type of incident. In ServiceCenter, problem type is a subcategory of Product type, enabling a more specific categorization of a problem for a particular product type. You can specify default problem types for Get-Services calls and incidents in the Get-Services tab of the Peregrine Portal Admin Module.

Product Type — a broad classification for devices, also known as device type. In ServiceCenter, product type is a subcategory of *subcategory*. You can specify default product types for Get-Services calls and incidents in the Get-Services tab of the Peregrine Portal Admin Module.

Request—Also known as problem. See *Incident*.

Severity —indicates how pressing an incident is for the caller. In ServiceCenter, severity level definitions are determined by an administrator. Default severity levels are: 1 - Critical; 2 - Urgent, 3 - Normal, 4 - Low, 5 - Very Low. You can specify default severity levels for Get-Services calls and incidents in the Get-Services tab of the Peregrine Portal Admin Module.

Site Category—the size of a site or campus location by number of users. In ServiceCenter, this alters the way the site is supported and on-site resources are allocated. Site category indicates the level of support provided. You can specify site categories for Get-Services calls and incidents in the Get-Services tab of the Peregrine Portal Admin Module.

Subcategory—further defines a call or incident, based on the primary category already selected. You can specify subcategories for Get-Services calls and incidents in the Get-Services tab of the Peregrine Portal Admin Module.

Index

Peregrine
SYSTEMS®

February 28, 2003