IBM Tivoli Identity Manager 4.6 Self Service Application Deployment and Customization Guide

Version 1.0

First Edition (May 2007)

Table of Contents

1

IBM Tivoli Identity Manager 4.6 Self Service Application

This paper describes the installation, configuration, and customization of IBM® Tivoli® Identity Manager Version 4.6 Self Service Application.

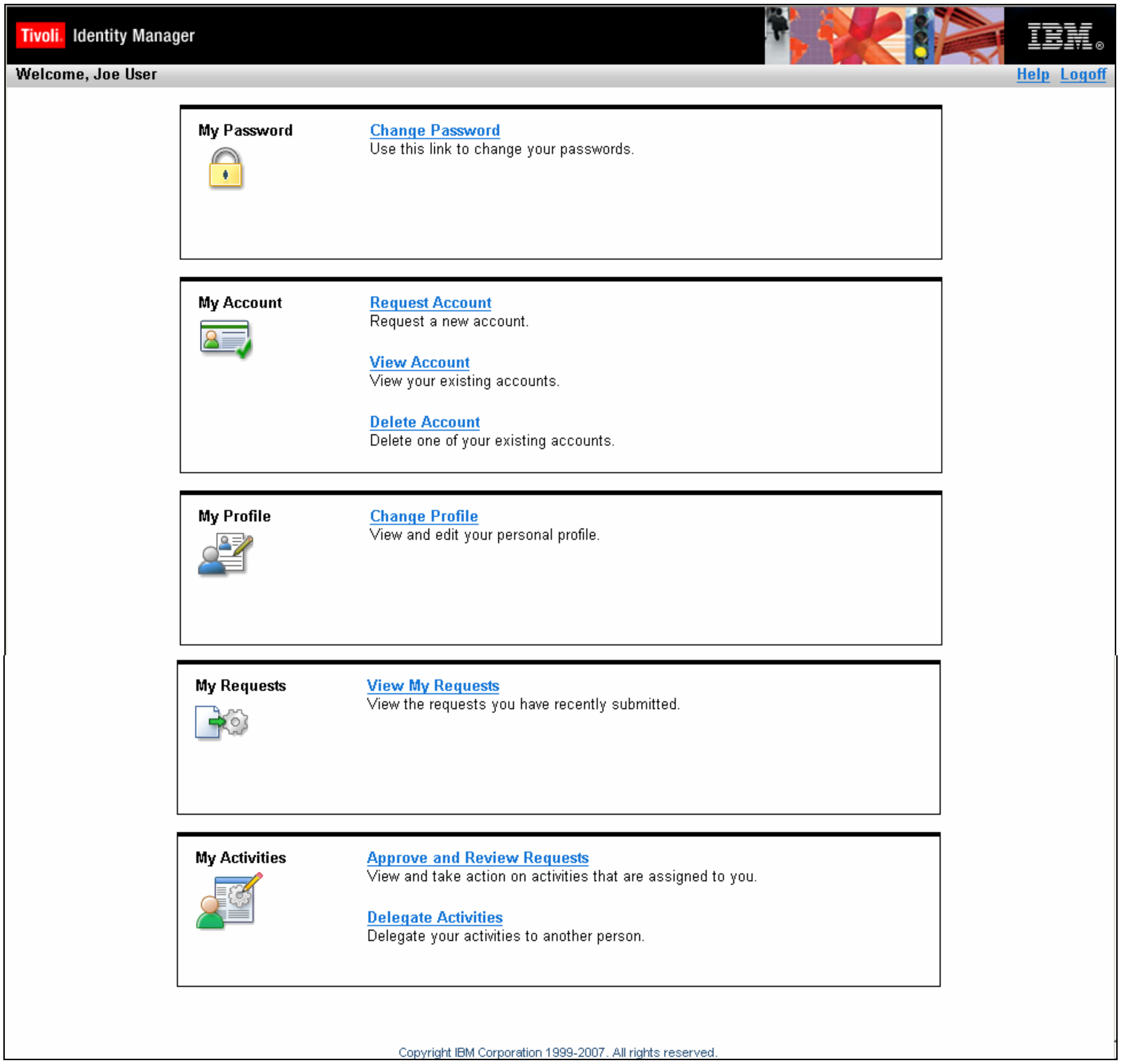
Overview

The IBM Tivoli Identity Manager 4.6 Self Service Application is an optional application to provide a simply, flexible user interface for customers.

Many customers implementing Tivoli Identity Manager into their environments want a simple user interface for their employees to use to interact with Tivoli Identity Manager to perform basic account management and provisioning functions. The ITIM 4.6 Self Service Application provides an optional user interface that customers may choose to use. The Self Service Application provides a simple, user friendly interface that is customizable and provides the basic Tivoli Identity Manager functions needed by end users.

The following self service functions can be enabled and disabled in the new user interface:

- Change Password
- Reset Password
- Request account
- Delete account
- View/change account
- View/Change Profile
- View Requests
- Approve and Review Activities
- Delegate Activities



My Password

Change Password
Use this link to change your passwords.

My Account

Request Account
Request a new account.

View Account
View your existing accounts.

Delete Account
Delete one of your existing accounts.

My Profile

Change Profile
View and edit your personal profile.

My Requests

View My Requests
View the requests you have recently submitted.

My Activities

Approve and Review Requests
View and take action on activities that are assigned to you.

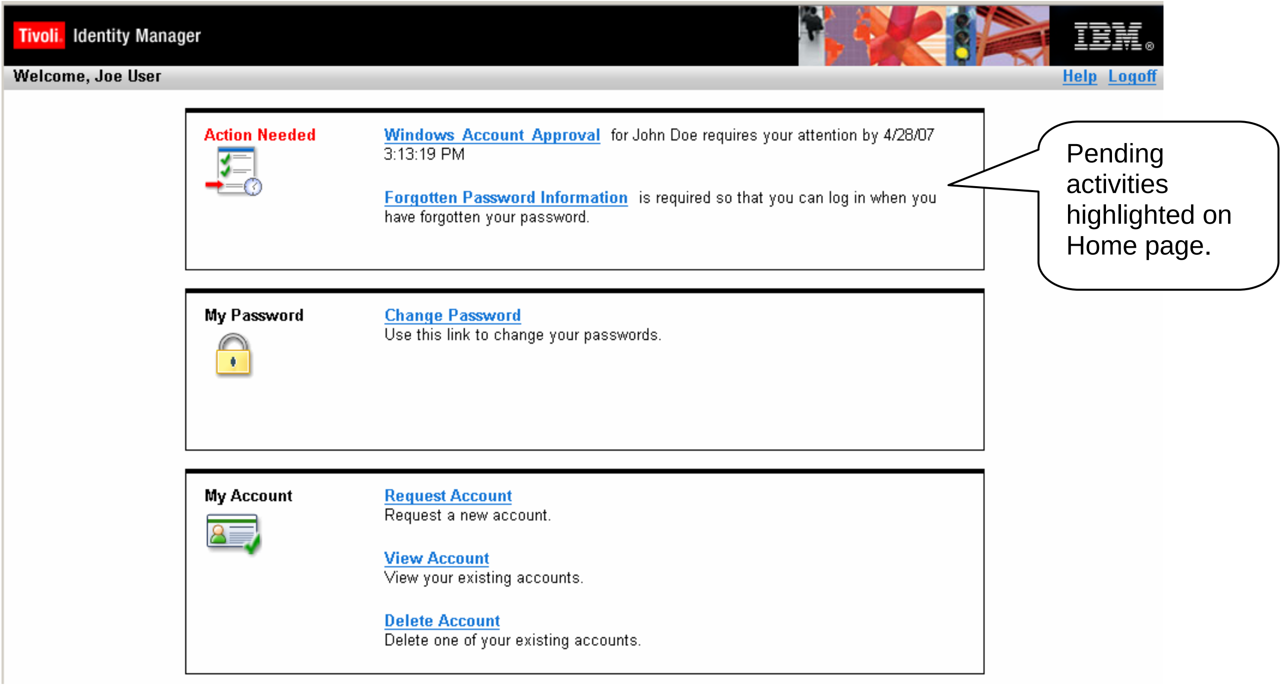
Delegate Activities
Delegate your activities to another person.

Copyright IBM Corporation 1999-2007. All rights reserved.

Figure 1: Self Service User Interface (all options displayed)

The Self Service Application also provides the following self-care functions to end users in a simple, easy-to-use user interface:

- Review/complete to-do activities
- Change forgotten password information
- Login using forgotten password information



Welcome, Joe User

Action Needed

Windows Account Approval for John Doe requires your attention by 4/28/07 3:13:19 PM

Forgotten Password Information is required so that you can log in when you have forgotten your password.

My Password

Change Password
Use this link to change your passwords.

My Account

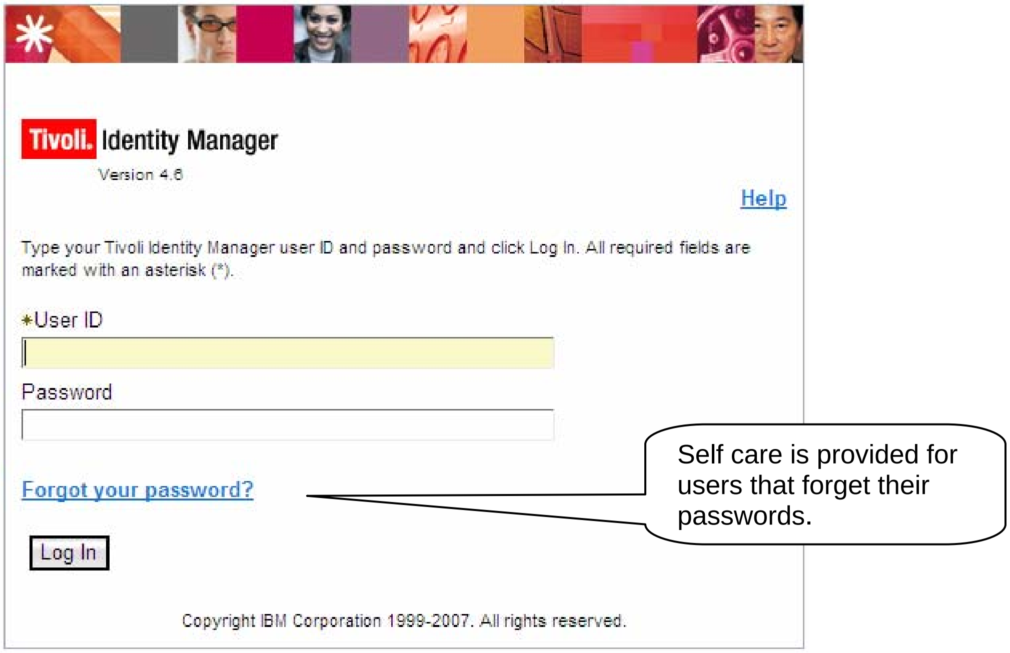
Request Account
Request a new account.

View Account
View your existing accounts.

Delete Account
Delete one of your existing accounts.

Pending activities highlighted on Home page.

Figure 2: Self Service UI with pending activities



Type your Tivoli Identity Manager user ID and password and click Log In. All required fields are marked with an asterisk (*).

*User ID

Password

Copyright IBM Corporation 1999-2007. All rights reserved.

Self care is provided for users that forget their passwords.

Figure 3: Logon with Challenge/Response Enabled

Many customization options are provided with the ITIM Self Service Application, giving customers the control and flexibility to manage how the Tivoli Identity Manager functions are presented to their employees. With the options provided, customers can integrate a self service user interface into their intranet website, maintaining their corporate look-and-feel.

2

Software Requirements

The following table provides the software prerequisites and the supported software environments for the ITIM 4.6 Self Service application.

Software	Supported Versions
Application Server	WebSphere 5.1.1
ITIM 4.6 maintenance	Fix pack 40 (4.6.0-TIV-TIM-FP0040) Interim fix 46 (4.6.0-TIV-TIM-IF0046)
Browser Support	Mozilla 1.7 Internet Explorer 6.0 with Service Pack 1

Limitations

- The ITIM Self Service Application must be deployed on the same WebSphere server/cluster instance as Tivoli Identity Manager 4.6 server.
- The ITIM Self Service Application supports English only (i.e. no translated language packs)
- The ITIM Self Service Application does not support the display of subforms on the account information forms.

  Subforms provide a means to submit an arbitrary number of parameter names and values for complex multi-valued attributes. Some adapters, such as those for RACF, PeopleSoft, SAP and TAM, include subforms. For account that use subforms, the standard account form will be displayed on the Self Service user interface but any attributes that use subforms will not be displayed. Data normally provided using the account information will have to be provided using other means.

3

ITIM Self Service Application Deployment

The deployment of the ITIM Self Service Application involves performing these steps:

1. Install the ITIM Self Service Application EAR file.

2. Create a WebSphere Shared Library for the ITIM Self Service Application containing the required IBM Tivoli Identity Manager JAR files.

3. Start the ITIM Self Service Application.

The deployment of the ITIM Self Service Application varies depending upon what WebSphere Configuration you are running: Single Server or Cluster.

Note: The ITIM Self Service Application is only supported on a WebSphere Single Server or WebSphere Cluster where the IBM Tivoli Identity Manager 4.6 Server is installed and running. Any other configuration is not supported.

Deploy the ITIM Self Service Application – Single Server Configuration

To deploy the ITIM Self Service Application in a WebSphere Single Server Configuration environment you will need to use the WebSphere Administration Console and perform the steps below.

1. Install the ITIM Self Service Application EAR file.

   - Unzip the archive file containing the ITIM Self Service Application code into the ***ITIM_HOME*** directory. Typically, the ***ITIM_HOME*** directory on a Windows operating system this will be **C:\Program Files\IBM\itim** and on a UNIX/Linux operating system it will be **/opt/IBM/itim**.

     Verify that the unzip operation placed the following files in the proper locations:

File	Location
itim_self_service.ear	***ITIM_HOME*** directory
SelfServiceHelp.properties	***ITIM_HOME/data*** directory
SelfServiceHomePage.properties	
SelfServiceScreenText.properties	
SelfServiceUI.properties	
SelfServiceView.properties	

   - Start the WebSphere administrative console

     http://<*hostname*>:9090/admin

The value of *hostname* is the fully qualified host name of the computer on which you installed the WebSphere Application Server.

- Click on the **Applications** group in the left frame, then click on the **Enterprise Applications** link, and then click on the **Install** button.

- If you started the WebSphere administrative console on the machine where the WebSphere Application Server is running select the **Local path** radio button and then click on the **Browse** button. Otherwise select the **Server path** radio button and then click on the **Browse** button.

- Using the File Dialog locate and select the file **itim_self_service.ear**. It should have been placed in the ***ITIM_HOME*** directory when you unzipped the archive file containing the ITIM Self Application code.

- Click on the **Next** button **five** times taking the defaults on each page.

- When you reach the last page the **Finish** button will appear. Click on the **Finish** button.

- When the install completes click on the **Save to Master Configuration** link.

- On the "**Save to Master Configuration**" page click on the **Save** button to update the WebSphere master repository.

2. Create the WebSphere Shared Library for the ITIM Self Service Application.

- Using the WebSphere administration console, click on the **Environment** group in the left frame.

- Click on the **Shared Libraries** link.

- Click on the **New** button.

- Specify these values for the following General Properties:

Name:	ITIM_SELFSERVICE_LIB
Classpath:	${APP_INSTALL_ROOT}/***node_name***/enRole.ear/itim_api.jar ${APP_INSTALL_ROOT}/***node_name***/enRole.ear/itim_server.jar ${APP_INSTALL_ROOT}/***node_name***/enRole.ear/app_ejb.jar ${APP_INSTALL_ROOT}/***node_name***/enRole.ear/wf_ejb.jar ${APP_INSTALL_ROOT}/***node_name***/enRole.ear/api_ejb.jar ${APP_INSTALL_ROOT}/***node_name***/enRole.ear/jlog.jar

In the **Classpath** entries above, substitute the text ***node_name*** with your WebSphere node name.

NOTE: Make sure there are no trailing blanks at the end of each line and that the entries are separated by the ENTER key. Trailing blanks may occur if the classpath information is cut-and-pasted from this document. If the classpaths are saved with trailing blanks, you will encounter "class not found" exceptions when using the Self Service user interface.

- After filling in the **Name** and **Classpath** property values, click on the **OK** button.

- Click on the **<u>Save</u>** link and then click on the **Save** button to update the WebSphere master repository.

You must now associate the Shared Library **ITIM_SELFSERVICE_LIB** with the ITIM Self Service Application. To make that association perform the following steps:

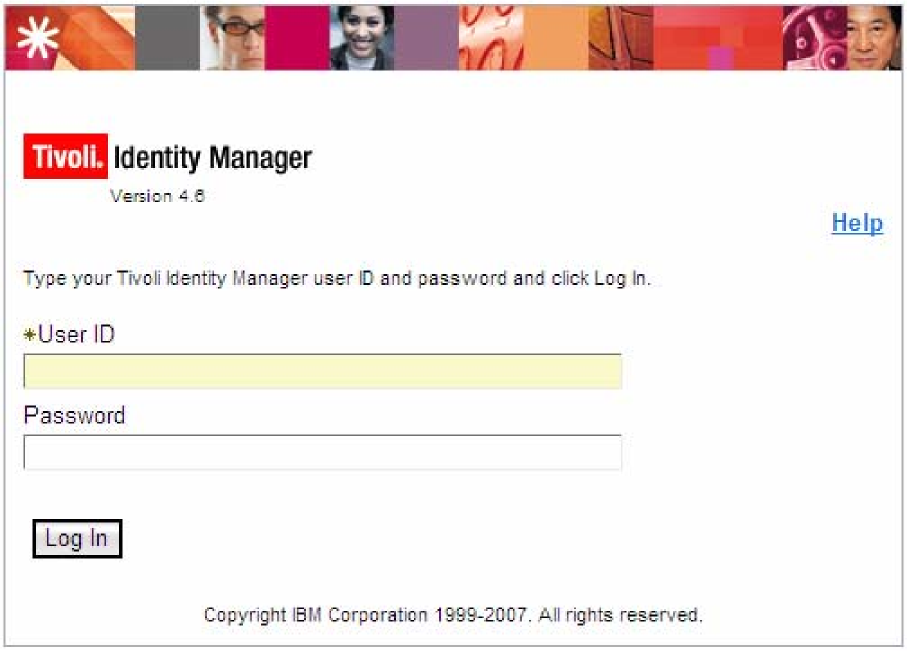
  - Click on the **Applications** group in the left frame.
  - Click on the **<u>Enterprise Applications</u>** link.
  - Click on the **<u>ITIM Self Service</u>** application link.
  - Under the "**Additional Properties**" section click on the **<u>Libraries</u>** link.
  - Click on the **Add** button.
  - Select the **ITIM_SELFSERVICE_LIB** entry in the **Library Name** drop-down list box. Click on the **OK** button.
  - Click on the **<u>Save</u>** link and then click on the **Save** button to update the WebSphere master repository.

3. Start the ITIM Self Service Application.

   - Using the WebSphere administration console, click on the **Applications** group in the left frame, and then click on the **<u>Enterprise Applications</u>** link.
   - Select the checkbox next to the **<u>ITIM Self Service</u>** application and click on the **Start** button.

4. Logon to the ITIM Self Service User Interface.

   http://<hostname>/itim/self



Type your Tivoli Identity Manager user ID and password and click Log In.

Copyright IBM Corporation 1999-2007. All rights reserved.

The ITIM Self Service logon page will be displayed. Enter a valid ITIM User ID and password.

Deploy the ITIM Self Service Application – Cluster Configuration

To deploy the ITIM Self Service Application in a WebSphere Cluster Configuration environment you will need to use the WebSphere Administration Console and perform the steps below.

1. Install the ITIM Self Service Application EAR file.

    - Unzip the archive file containing the ITIM Self Service Application code into the ***ITIM_HOME*** directory. Typically, ***ITIM_HOME*** directory on a Windows operating system this will be **C:\Program Files\IBM\itim** and on a UNIX/Linux operating system it will be **/opt/IBM/itim**.

      Verify that the unzip operation placed the following files in the proper locations:

File	Location
itim_self_service.ear	***ITIM_HOME*** directory
SelfServiceHelp.properties	***ITIM_HOME/data*** directory
SelfServiceHomePage.properties	
SelfServiceScreenText.properties	
SelfServiceUI.properties	
SelfServiceView.properties	

> **NOTE:** In a clustered environment, the Self Service properties files from the archive file (listed above) need to be copied into the ***ITIM_HOME/data*** directories on all servers in the cluster that will run the ITIM Self Service Application.

- Start the WebSphere administrative console

  http://<*hostname*>:9090/admin

  The value of *hostname* is the fully qualified host name of the computer on which you installed the WebSphere Deployment Manager.

- Click on the **Applications** group in the left frame, then click on the **Enterprise Applications** link, and then click on the **Install** button.

- If you started the WebSphere administrative console on the machine where the WebSphere Deployment Manager is running select the **Local path** radio button and then click on the **Browse** button. Otherwise select the **Server path** radio button and then click on the **Browse** button.

- Using the File Dialog locate and select the file **itim_self_service.ear**. It should have been placed in the ***ITIM_HOME*** directory when you unzipped the archive file containing the ITIM Self Application code.

- Click on the **Next** button **four** times taking the defaults on each page.

- On “Step 3: Map modules to application servers” use the “Clusters and Servers:” list box to select the name of the clusters and servers on which to install the application. Click on **Apply.**

- When you reach the last page the **Finish** button will appear. Click on the **Finish** button.

- On the “**Save to Master Configuration**” page ensure that the “**Synchronize changes with Nodes**” checkbox is selected and then click on the **Save** button to update the WebSphere master repository.

2. Create the WebSphere Shared Library for the ITIM Self Service Application.

   - Using the WebSphere administration console, click on the **Environment** group in the left frame.

   - Click on the **Shared Libraries** link.

   - You will be defining the Shared Library at the **Cell** scope. Clear the **Node** and **Server** edit boxes (if they contain any values) and then click on the **Apply** button.

   - Click on the **New** button.

   - Specify these values for the following General Properties:

Name: ITIM_SELFSERVICE_LIB

Classpath:
${APP_INSTALL_ROOT}/***cell_name***/enRole.ear/itim_api.jar
${APP_INSTALL_ROOT}/***cell_name***/enRole.ear/itim_server.jar
${APP_INSTALL_ROOT}/***cell_name***/enRole.ear/app_ejb.jar
${APP_INSTALL_ROOT}/***cell_name***/enRole.ear/wf_ejb.jar
${APP_INSTALL_ROOT}/***cell_name***/enRole.ear/api_ejb.jar
${APP_INSTALL_ROOT}/***cell_name***/enRole.ear/jlog.jar

In the **Classpath** entries above, substitute the text ***cell_name*** with the WebSphere cell name.

NOTE: Make sure there are no trailing blanks at the end of each line and that the entries are separated by the ENTER key. Trailing blanks may occur if the classpath information is cut-and-pasted from this document. If the classpaths are saved with trailing blanks, you will encounter “class not found” exceptions when using the Self Service user interface.

   - After filling in the **Name** and **Classpath** property values, click on the **OK** button.

   - Click on the **Save** link and then click on the **Save** button to update the WebSphere master repository.

You must now associate the Shared Library **ITIM_SELFSERVICE_LIB** with the ITIM Self Service Application. To make that association perform the following steps:

- Click on the **Applications** group in the left frame.

- Click on the **Enterprise Applications** link.

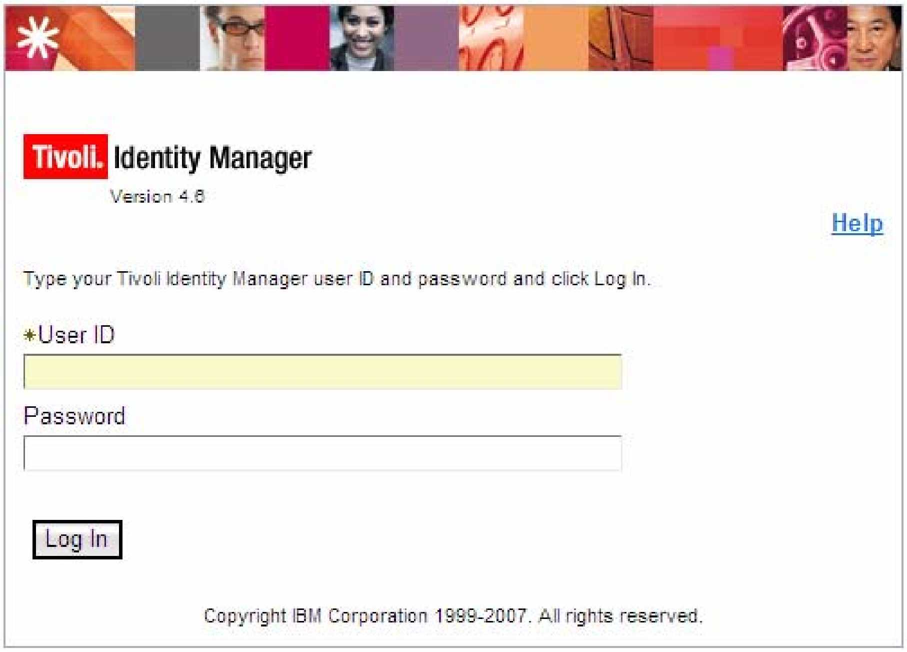
   - Click on the **ITIM Self Service** application link.
   - Under the “**Additional Properties**” section click on the **Libraries** link.
   - Click on the **Add** button.
   - Select the **ITIM_SELFSERVICE_LIB** entry in the **Library Name** drop-down list box. Click on the **OK** button.
   - Click on the **Save** link and then click on the **Save** button to update the WebSphere master repository.

3. Update Web Server Plug-in
   - Using the WebSphere administration console on the Deployment Manager, click on the **Environment** group in the left frame, and then click on the **Update Web Server Plug-in** link.
   - Click on **OK** button

4. Start the ITIM Self Service Application.
   - Using the WebSphere administration console, click on the **Applications** group in the left frame, and then click on the **Enterprise Applications** link.
   - Select the checkbox next to the **ITIM Self Service** application and click on the **Start** button.

5. Logon to the ITIM Self Service User Interface.

   http://<hostname>/itim/self



Type your Tivoli Identity Manager user ID and password and click Log In.

Copyright IBM Corporation 1999-2007. All rights reserved.

The ITIM Self Service logon page will be displayed. Enter a valid ITIM User ID and password.

Re-installing the ITIM Self Service Application

If you need to re-install the ITIM Self Service Application due to applying a fix pack or interim fix, you will need to first stop the application and then uninstall it. You can then follow the previous installation instructions.

If you have customized any of the ITIM Self Service Application property files you should back them up before re-installing the ITIM Self Service Application. After re-installing the ITIM Self Service Application you will need to merge your changes back into the newly installed files. These files include the following files and any other files you might have changed (style sheets, etc.).

ITIM_HOME/data/SelfServiceHelp.properties
ITIM_HOME/data/SelfServiceHomePage.properties
ITIM_HOME/data/SelfServiceScreenText.properties
ITIM_HOME/data/SelfServiceUI.properties
ITIM_HOME/data/SelfServiceView.properties

Stopping and Uninstalling the ITIM Self Service Application in a Single Server Configuration

- Using the WebSphere administration console, click on the **Applications** group in the left frame, and then click on the **Enterprise Applications** link.
- Select the checkbox next to the **ITIM Self Service** application and click on the **Stop** button.
- When the Stop completes, select the checkbox next to the **ITIM Self Service** application and click on the **Uninstall** button.
- When the Uninstall completes click on the **Save** link.
- On the "**Save to Master Configuration**" page click on the **Save** button to update the WebSphere master repository.

Stopping and Uninstalling the ITIM Self Service Application in a Cluster Configuration

- Using the WebSphere administration console, click on the **Applications** group in the left frame, and then click on the **Enterprise Applications** link.
- Select the checkbox next to the **ITIM Self Service** application and click on the **Stop** button.
- When the Stop completes, select the checkbox next to the **ITIM Self Service** application and click on the **Uninstall** button.
- When the Uninstall completes click on the **Save** link.
- On the "**Save to Master Configuration**" page ensure that the "**Synchronize changes with Nodes**" checkbox is selected and then click on the **Save** button to update the WebSphere master repository.

Install the new release of the ITIM Self Service Application and restore backup files

Go to the ITIM Self Service Deployment sections and follow the steps to deploy the new release of the Self Service Application. After completing the re-installation of the ITIM Self Service Application, restore any files that you have backed up.

4

Configuration Options

Configuration Files

The ITIM Self Service Application delivers several property files that control the options, layout and text that are displayed on the user interface. These files are stored in the **<ITIM_HOME>/data** directory when the archive file is unzipped into the ***ITIM_HOME*** directory

The files are:

- SelfServiceView.properties
  Defines view definitions for groups using the user interface.
- SelfServiceUI.properties
  Controls the layout of the user interface (header, footer, navigation bar, left frame) and the number of pages displayed, search results returned
- SelfServiceScreenText.properties
  Provides the text that is displayed on the Self Service user interface
- SelfServiceHomePage.properties
  Defines the sections of the home page in the order they will be displayed
- SelfServiceHelp.properties
  Defines the links to html help pages that appear on the Self Service user interface. The html files are located in the itim_self_service.war file (located in the WebSphere directory; ${APP_INSTALL_ROOT}/***node_name***/ITIM_Self_Service.ear/)

When the archive file containing the ITIM Self Service Application code is unzipped, a **defaults** directory is created containing the original, default copies of customizable files.

Original versions of the above property files are stored in the **<ITIM_HOME>/defaults/data** directory. If there is ever a need to revert back to the original configuration of the Self Service user interface, use these files to replace the customized files.

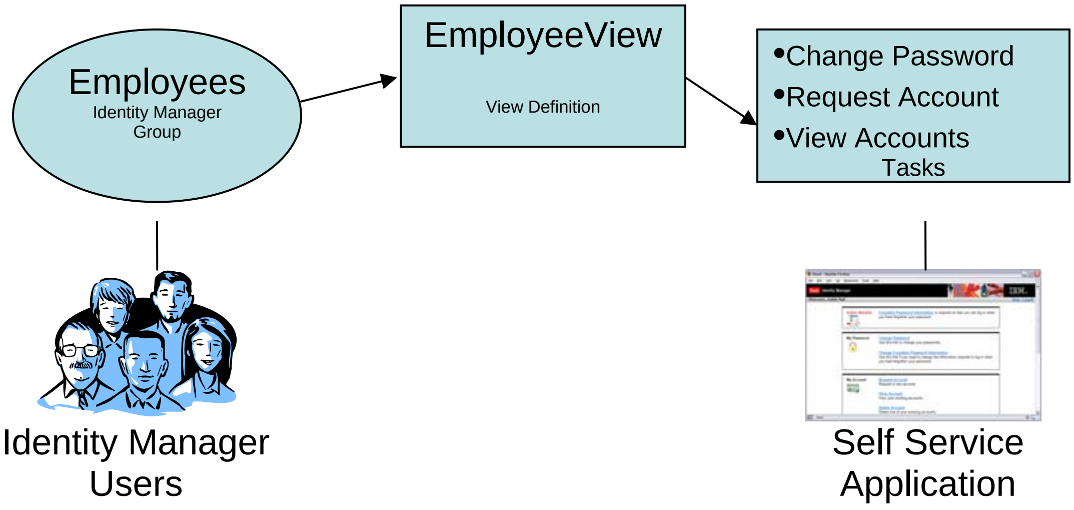
In addition to the five files listed above, a file called **SelfServiceScreenTextKeys.properties** is also included in this directory. This file provides label keys that are displayed on the Self Service user interface. This file can be used to assist with customization of screen text. The section titled ‘Determining the Key for a Screen Label’ provides details on how this file can be used.

Configuring which tasks are displayed in the Self Service application

The self service application can display different tasks based on the user that is logged in. View definitions allow you to configure which tasks are available to a group of users. View definitions for the Self Service application are configured in the **SelfServiceView.properties** file. This section will discuss how to configure view definitions, how view definitions change the user interface, and how view definitions interact with Access Control Items (ACIs).

What are View Definitions?

A view definition is a simple mapping between a group of Identity Manager Users and the list of tasks they are allowed to access in the Self Service application.



Concepts

- Views: defines the tasks a given group of users will have access to through the Self Service Application

- Tasks: the high level functions available from the Self Service Application such as Change Password and Request Account

- Identity Manager Groups: Groups a set of Identity Manager user accounts.

Configuring View Definitions

The steps involved for configuring view definitions for the Self Service Application are:

1. Define Tivoli Identity Manager groups through the administration console (Provisioning → Manage ITIM Groups)
2. Assign users to the groups
3. Update/Add entries to the **SelfServiceView.properties** file.

View definitions for the Self Service application are configured in the **SelfServiceView.properties** file.

A View Definition entry has the following format:

File format:

<ViewName>.groups=***<group name1>,<group name2>, …***
<ViewName>.tasks=***<TaskID 1>, <TaskID 2>, …***

Where:

<ViewName> is a name provided by the administrator to identify a view definition

<group name> represents the name of a defined Tivoli Identity Manager group.

- Multiple group names separated by commas can be listed on a View definition.
- An asterisk (*) is used to define the default view. The default view is the list of tasks given to all users not governed by a specific view.
- The asterisk can be included in the list of groups for one view. For example:
  Test.groups=TestGroup1,TestGroup2,*

<TaskID> is an ID from the task list in Table 1: Configuring Features in SelfServiceView.propertiesTable 1: Configuring Features in SelfServiceView.properties below.

Additional notes regarding ***<group name>*** definitions:

- ***<group name>*** is case sensitive. Be sure each ***<group name>*** specified in this file matches a defined Tivoli Identity Manager group.
- Groups can only be associated with one view.
- If users belong to multiple groups that appear in different view definitions, the user will be granted the union of all tasks in the relevant view definitions.
- If a user is a member of a group that has an assigned view, the * is not applicable to that user.
- Only comma delimiters are supported to separate group names.

Feature	**Task ID**	**Description**
Change Password	CHANGE_PASSWORDS	Allows user to change passwords for accounts they own.
Request Account (basic)	MANAGE_MY_ACCOUNTS-REQUEST_ACCOUNT	Allows user to view the request account feature, showing a list of all accounts the user can request The list of accounts displayed to the user is controlled by provisioning policy and the Account 'Add' ACI.
Request Account (advanced)	MANAGE_MY_ACCOUNTS-REQUEST_ACCOUNT_ADVANCED	Allows user to view the request account feature, showing a search page to search for accounts the user can request. The accounts returned as a result of the search criteria are controlled by the provisioning policy and the Account 'Add' ACI. **NOTE:** If the user has both MANANGE_MY_ACCOUNTS-REQUEST_ACCOUNT and MANAGE_MY_ACCOUNTS-REQUEST_ACCOUNT_ADVANCED, the advanced view will be displayed.

Feature	**Task ID**	**Description**
View Account	MANAGE_MY_ACCOUNTS-VIEW_ACCOUNT	Allows user to view the accounts they own and on which the ‘Search’ ACI is granted. The user will be allowed to view a ‘read only’ account form. The form will be ‘read only’ even if the user is granted the Account ‘Modify’ ACI.
Change Account	MANAGE_MY_ACCOUNTS-CHANGE_ACCOUNT	Allows user to request changes to the accounts they own and on which the Account ‘Search’ and Account ‘Modify’ ACIs are granted. Accounts that the user is only allowed to search will not be displayed.
View or Change Account	MANAGE_MY_ACCOUNTS-VIEW_ACCOUNT, MANAGE_MY_ACCOUNTS-CHANGE_ACCOUNT	If the user is granted the task IDs for both View and Change account then the ‘View or Change Account’ task will be available. Allows user to view and request changes to accounts. All accounts on which the user is granted the Account ‘Search’ ACI will be shown. When an account is selected, a read only or editable form will be displayed based whether the user is granted the Account ‘Modify’ ACI on the specified account.
Delete Account	MANAGE_MY_ACCOUNTS-DELETE_ACCOUNT	Allows user to request deletion of accounts they own. Accounts on which the user is granted the Account ‘Search’ and ‘Remove’ Account ACIs will be displayed.
View Profile	VIEW_PERSONAL_PROFILE	Allows user to view their personal profile. The user must be granted the Person ‘Search’ ACI in order to view their profile. The user will be shown a ‘read only’ person profile form even if the user is granted the Person ‘Modify’ ACI.

Feature	**Task ID**	**Description**
Change Profile	CHANGE_PERSONAL_PROFILE	Allows user to change their personal profile if they are granted the Person ‘Search’ and Person ‘Modify’ ACIs. If the user is granted Person ‘Search’ ACI but not modify then a read only form will be displayed.
View or Change Profile	VIEW_PERSONAL_PROFILE, CHANGE_PERSONAL_PROFILE	The same as Change Profile task from an ACI perspective. The titles of the task will change to show View or Change Profile
View Requests	VIEW_REQUESTS-VIEW_ALL_MY_REQUEST	Allows user to view the history of the requests they have made.
Review Activities	VIEW_TODO_LIST	Allows the user to work with Approvals, RFIs, Work Orders and Compliance Alerts they have been assigned. **Note** if the user is not granted the Review Activities task but, they have Activities assigned to them, they will still be able to access the Review Activities view via the Action Needed section.
Delegate Activities	DELEGATE_TODOS	Allows users to delegate processing of their Activities to other users. The user needs to be granted the ‘Delegate’ ACI. To enable searching for people to delegate activities to, the Person ‘Search’ ACI must be enabled for the user.
Change Forgotten Password Information	Not governed by View Definitions	Allows users to set their forgotten password questions. This task is not controlled by define views but will be displayed if Challenge Response is enabled and configured in the Identity Manager Console.
Action Needed	Not governed by View Definitions	Alerts user to actions that require their attention such as Approvals, RFIs or setting forgotten password information.

Table 1: Configuring Features in SelfServiceView.properties

Access Control Items (ACIs)

Access Control Items (ACIs) are key elements in determining whether features of the Self Service user interface will operate properly.

ACIs are defined by a Tivoli Identity Manager administrator. There are three basic ACIs that impact how the Self Service features operate: Account ACI, Person ACI and Identity Manager User ACI. These three ACIs are defined by going to ‘My Organization’ and then selecting ‘Control Access’.

One other ACI, a Service ACI, is needed to allow end users to view the service description when they are requesting new accounts. This Service ACI is defined by selecting ‘Provisioning’ and then selecting ‘Control Access’.

Description	Description	ACI Category	Operation
Account ‘Search’ ACI	Needed for ‘View’, ‘Change’ and ‘Delete Account’ features.	Account ACI (defined under ‘My Organization’)	Search
Account ‘Modify’ ACI	Needed for ‘Change Account’ feature.		Modify
Account ‘Add’ ACI	Needed for ‘Request Account’ feature.		Add
Account ‘Delete’ ACI	Needed for ‘Delete Account’ feature.		Remove
Person ‘Search’ ACI	Needed for ‘Delegate Activities’ feature	Person ACI (defined under ‘My Organization’)	Search
Person ‘Modify’ ACI	Needed for ‘Change Profile’ feature		Modify
‘Delegate ACI’	Needed for ‘Delegate Activities’ feature	Identity Manager User ACI (defined under ‘My Organization’)	Search (with Attribute Permission = Delegate)
‘Service’ ACI	Needed to display service descriptions when end users ‘Request Accounts’	Service ACI (defined under ‘Provisioning’)	Search

Table 2: ACIs Needed for Self Service Features

For more details and examples regarding ACIs, see Appendix A.

Example View Definitions:

```
#Grants Change Password, View Account, View Profile, and View Requests
#to all users not governed by another view
BasicUserView.groups=*
BasicUserView.tasks=CHANGE_PASSWORDS, MANAGE_MY_ACCOUNTS-VIEW_ACCOUNT,
VIEW_PERSONAL_PROFILE, VIEW_REQUESTS-VIEW_ALL_MY_REQUEST

#Grants Change Password, Request Account,  View or Change Account,
#View Profile, and View Requests to all users in the Employees
#and Contractor Identity Manager Groups
EmployeeView.groups=Employees,Contractors
EmployeeView.tasks=CHANGE_PASSWORDS, MANAGE_MY_ACCOUNTS-VIEW_ACCOUNT,
MANAGE_MY_ACCOUNTS-CHANGE_ACCOUNT, VIEW_PERSONAL_PROFILE, MANAGE_MY_ACCOUNTS-
REQUEST_ACCOUNT, VIEW_REQUESTS-VIEW_ALL_MY_REQUEST
```

In the simple example above, two views are defined. One view, **EmployeeView**, is for users that belong to the ITIM groups ‘Employees’ or ‘Contractors’. The tasks they are able to see on the Self Service user interface are defined by **EmployeeView.tasks=…** .

The second view, **BasicUserView**, will apply to all users that do not belong to either the ‘Employees’ or ‘Contractors’ ITIM groups. This could be called the ‘default’ view since it will apply to users that are not governed by a view for a specific group.

How a User’s Tasks are Determined

When a user logs into the Self Service application, their current group membership is compared with view definitions to determine the list of Tasks that should be displayed. The basic rules for determining which tasks the user can access are:

1. If the user is not a member of a group or if the user is a member of a group that is not associated with a view, then the user will be granted the default view (i.e. the view defined with the “*” value). This default view is for users that are not governed by another view.
2. If the user is a member of a group associated with a view, they will be granted the tasks defined for that view.
3. If the user is a member of multiple groups associated with multiple views, they will be granted the union of the tasks associated with those views.

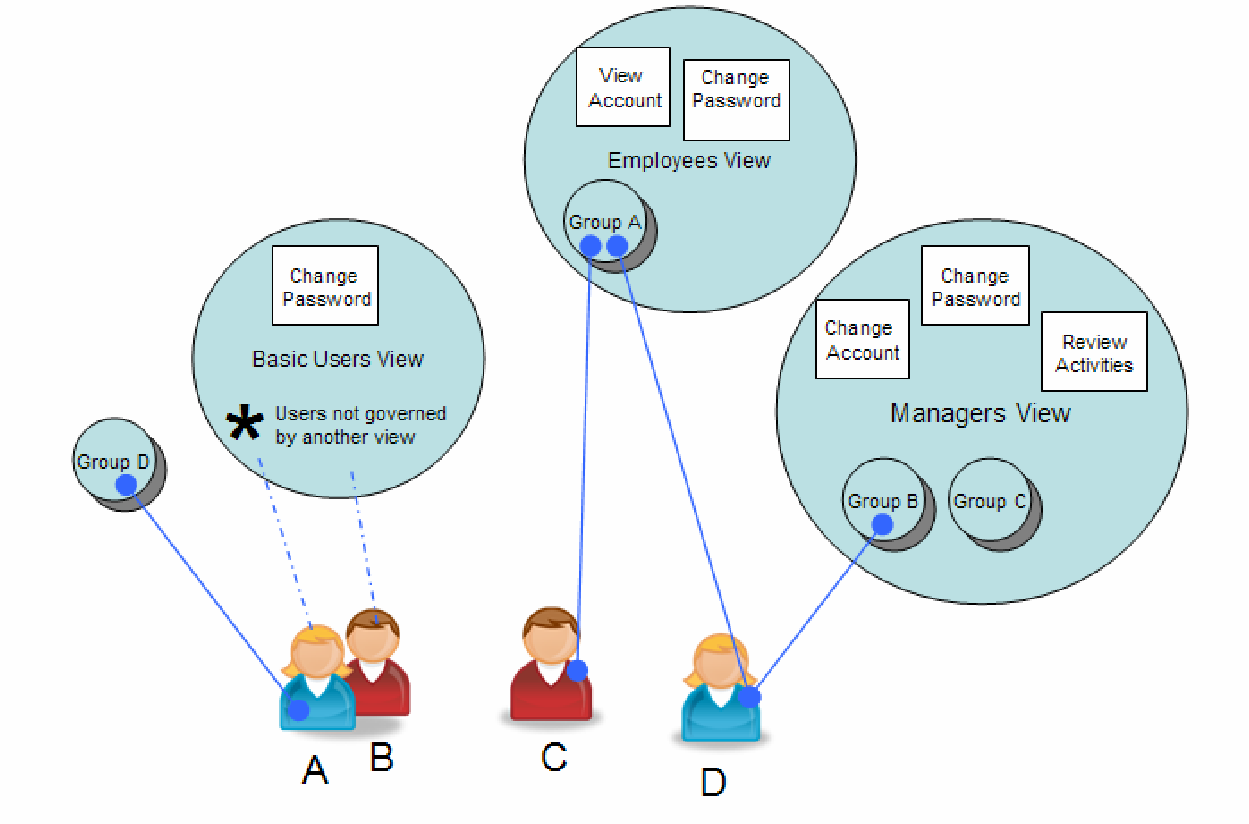


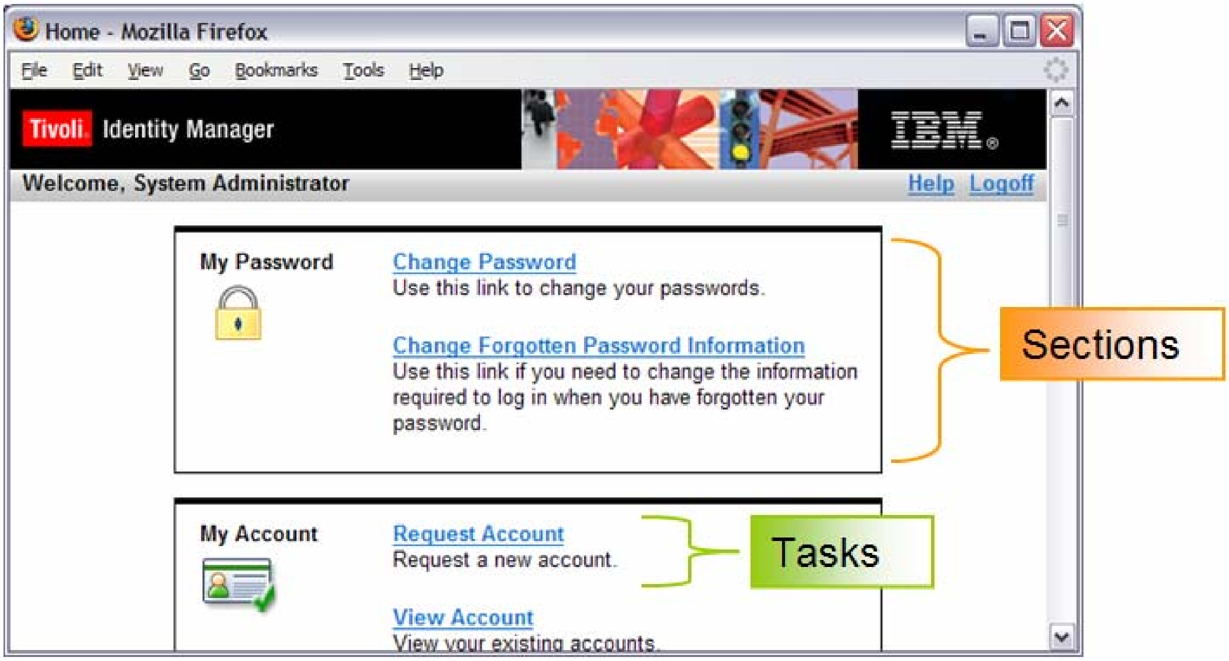
Figure 4: Task Determination Example

User	Tasks	Description
A	Change Password	User A is a member of Group D, but Group D is not associated with any views, therefore user A is granted the "default" view.
B	Change Password	User B is not a member of any groups and therefore granted the "default" view.
C	View Account, Change Password	User C is a member of Group A which is mapped to the Employees View. The Employees view grants View Account and Change Password.
D	View or Change Account, Change Password, Review Activities	User D is a member of multiple groups associated with multiple views. Therefore User D is granted tasks for both the Employees and Managers views.

User Interface elements affected by Views.

Home Page

The home page adapts to the user's views by only showing the tasks on the home page that the user is granted. If the user is not allowed to view any task in a section, then the section will also be removed from the home page. If the user has both 'Change' and 'View' tasks for account or profile, it will combine them into a single task.



Welcome, System Administrator

My Password

Change Password
Use this link to change your passwords.

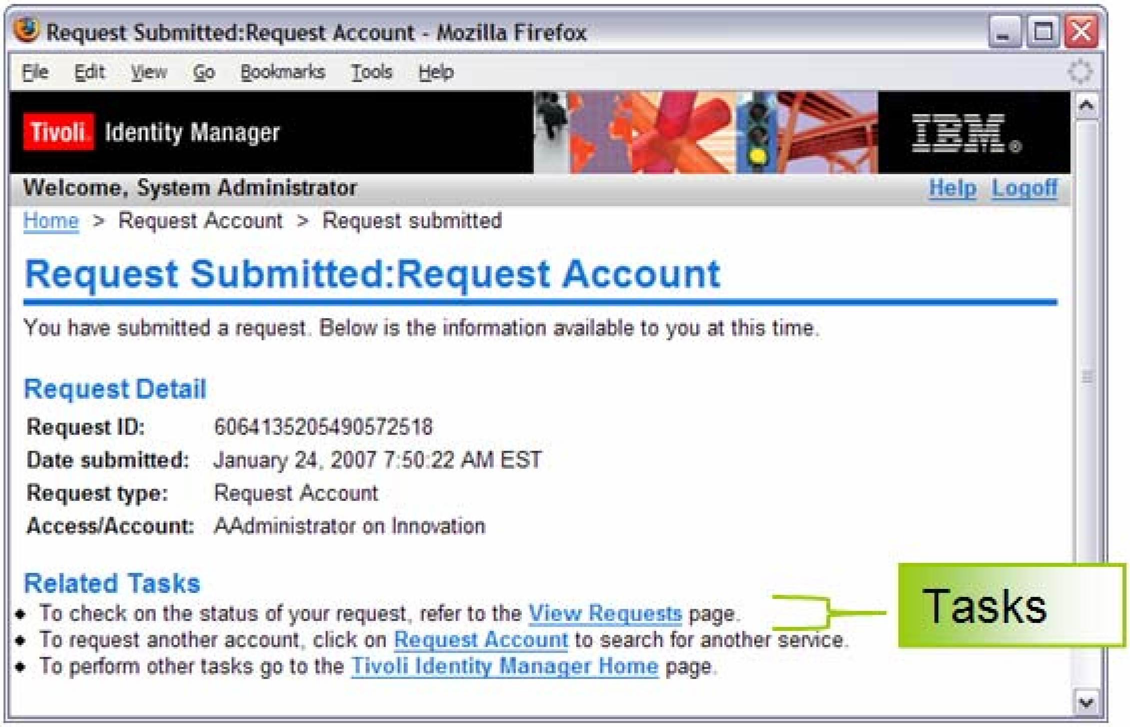
Change Forgotten Password Information
Use this link if you need to change the information required to log in when you have forgotten your password.

My Account

Request Account
Request a new account.

View Account
View your existing accounts.

Related Tasks
In many areas of the Self Service application, related task sections are displayed. These sections are also filtered by view definitions. For example if the user does not have access to ‘View Requests’, then it will be filtered from the ‘Related Tasks’ section.


Request Submitted:Request Account - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
Tivoli. Identity Manager
IBM.
Help Logoff
Tasks

Welcome, System Administrator

Home > Request Account > Request submitted

Request Submitted:Request Account

You have submitted a request. Below is the information available to you at this time.

Request Detail

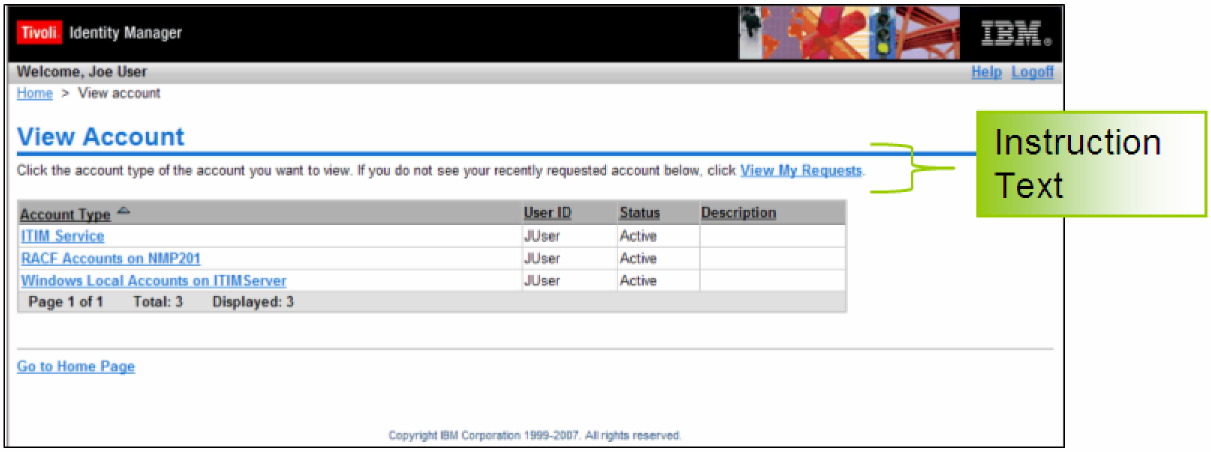
Request ID: 6064135205490572518
Date submitted: January 24, 2007 7:50:22 AM EST
Request type: Request Account
Access/Account: AAdministrator on Innovation

Related Tasks

- To check on the status of your request, refer to the View Requests page.
- To request another account, click on Request Account to search for another service.
- To perform other tasks go to the Tivoli Identity Manager Home page.

Panel Instruction Text

The instruction text on certain screens may contain links to the 'View Requests' task.   A different instruction message will be displayed without the task link if the user is not granted the View Requests task.



View Account

Click the account type of the account you want to view. If you do not see your recently requested account below, click View My Requests.

Account Type	User ID	Status	Description
ITIM Service	JUser	Active	
RACF Accounts on NMP201	JUser	Active	
Windows Local Accounts on ITIMServer	JUser	Active	

Page 1 of 1   Total: 3   Displayed: 3

Go to Home Page

Copyright IBM Corporation 1999-2007. All rights reserved.

5

Customization

The Self Service application can be customized to blend into existing internet sites. This chapter will discuss the following customization options supported by the Self Service application:

- Changing labels, instructions, and text presented in the user interface
- Customizing website layout, Banner, Footer, Toolbar, and Left Navigation bar
- Customizing the Home Page
- Look and Feel customization using Cascading Style Sheets (CSS)
- Replacing on-line help content.

Some aspects of customizing the Self Service application are relatively easy. Customizations can be made by understanding the Self Service ***.properties*** files and making the appropriate modifications. Other aspects of customization are more complex and require knowledge and experience with Cascading Style Sheets (CSS) and/or JavaServer Pages (JSP).

Only the files located in the deployed WebSphere directory can be customized:

<WAS_HOME>/installedApps/<nodeName>/ITIM_Self_Service.ear/itim_self_service.war/custom/

Only the following files contained in the **itim_self_service.war/custom** directory can be customized:

Cascading Style Sheets (CSS files)	JavaServer Pages (JSP files)
end_user.css end_user_rtl.css widgets.css widgets_rtl.css date_Widget_ltr.css date_Widget_rtl.css time.css calendar.css customForm.css customForms_rtl.css	banner.jsp footer.jsp home.jsp nav.jsp toolbar.jsp

Table 3. Customizable CSS and JSP files

When the archive file containing the ITIM Self Service Application code is unzipped, a **defaults** directory is created containing the original, default copies of these customizable files.

Original versions of the customizable CSS and JSP files (see Table 3. Customizable CSS and JSP files) are stored in the **<ITIM_HOME>/defaults/custom** directory.

Original versions of the following property files are stored in the **<ITIM_HOME>/defaults/data** directory.

- SelfServiceHelp.properties

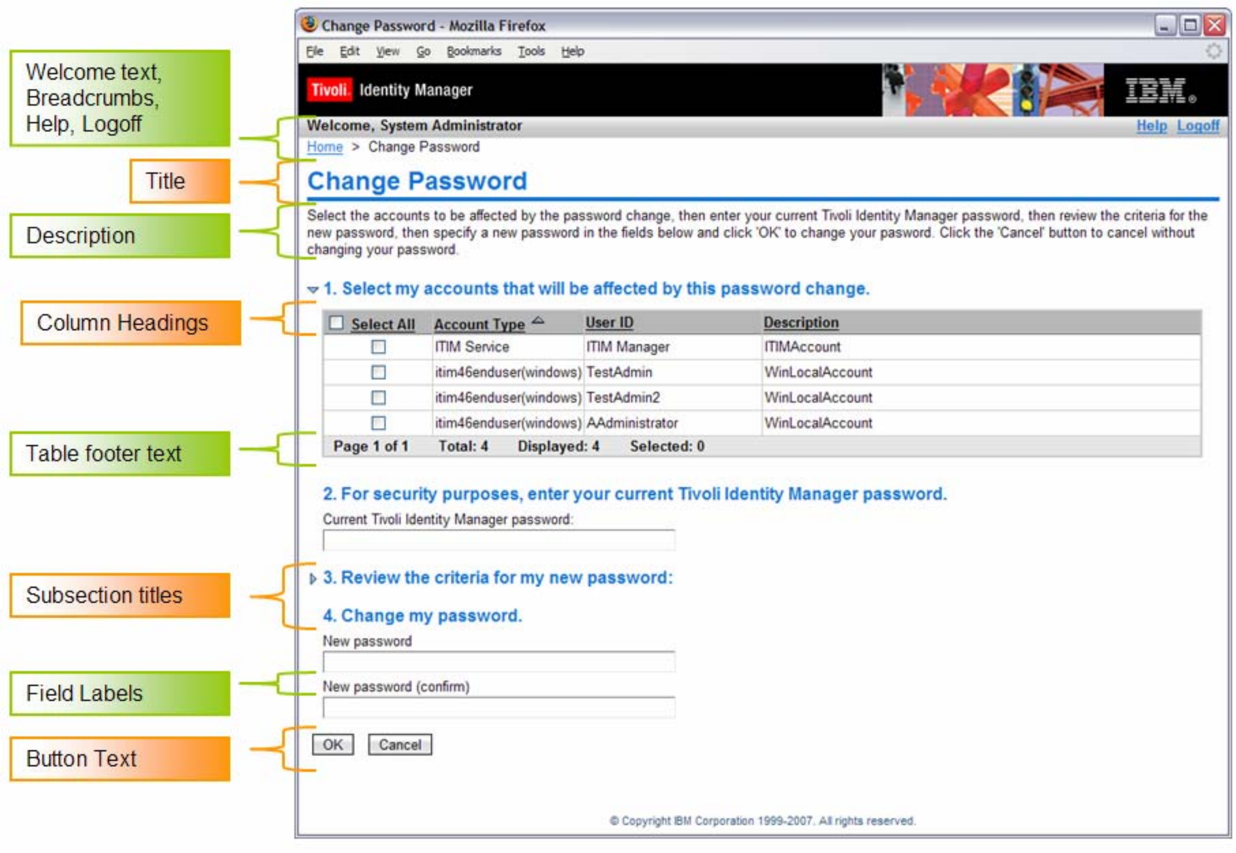
- SelfServiceHomePage.properties
- SelfServiceScreenText.properties
- SelfServiceScreenTextKeys.properties
- SelfServiceUI.properties
- SelfServiceView.properties

If there is ever a need to revert back to the original configuration of the Self Service user interface, use these files to replace the customized files.

Changing Labels, Description, and other Screen Text

The majority of the text displayed in the Self Service application can be replaced via customization. The following items can be updated:

- Titles
- Subsection titles
- Page / Subsection descriptions
- Field Labels
- Table column headers/footer
- Button text



Welcome, System Administrator

Home > Change Password

Change Password

Select the accounts to be affected by the password change, then enter your current Tivoli Identity Manager password, then review the criteria for the new password, then specify a new password in the fields below and click 'OK' to change your pasword. Click the 'Cancel' button to cancel without changing your password.

1. Select my accounts that will be affected by this password change.

☐ Select All	Account Type	User ID	Description
☐	ITIM Service	ITIM Manager	ITIMAccount
☐	itim46enduser(windows)	TestAdmin	WinLocalAccount
☐	itim46enduser(windows)	TestAdmin2	WinLocalAccount
☐	itim46enduser(windows)	AAdministrator	WinLocalAccount

Page 1 of 1 Total: 4 Displayed: 4 Selected: 0

2. For security purposes, enter your current Tivoli Identity Manager password.

Current Tivoli Identity Manager password:

3. Review the criteria for my new password:

4. Change my password.

New password

New password (confirm)

© Copyright IBM Corporation 1999-2007. All rights reserved.

Figure 5: Screen Text

Editing Screen Text

Titles, Descriptions, Subsections, Buttons…

The primary source for screen text in the Self Service application is in Java Properties resource bundle format. The resource bundle is named: **SelfServiceScreenText.properties** and was copied into the **<ITIM_HOME>/data** directory during installation of the Self Service application. This properties file contains key / value pairs for labels related to title, description, subsection titles, table column headers / footers, buttons and other text shown in Figure 5: Screen Text.

Take the following steps to update the screen text:

1. To preserve the current screen text, make a backup copy of the **SelfServiceScreenText.properties** file.

2. Edit the **SelfServiceScreenText.properties** file. Modify the values of the screen text fields and save the file.

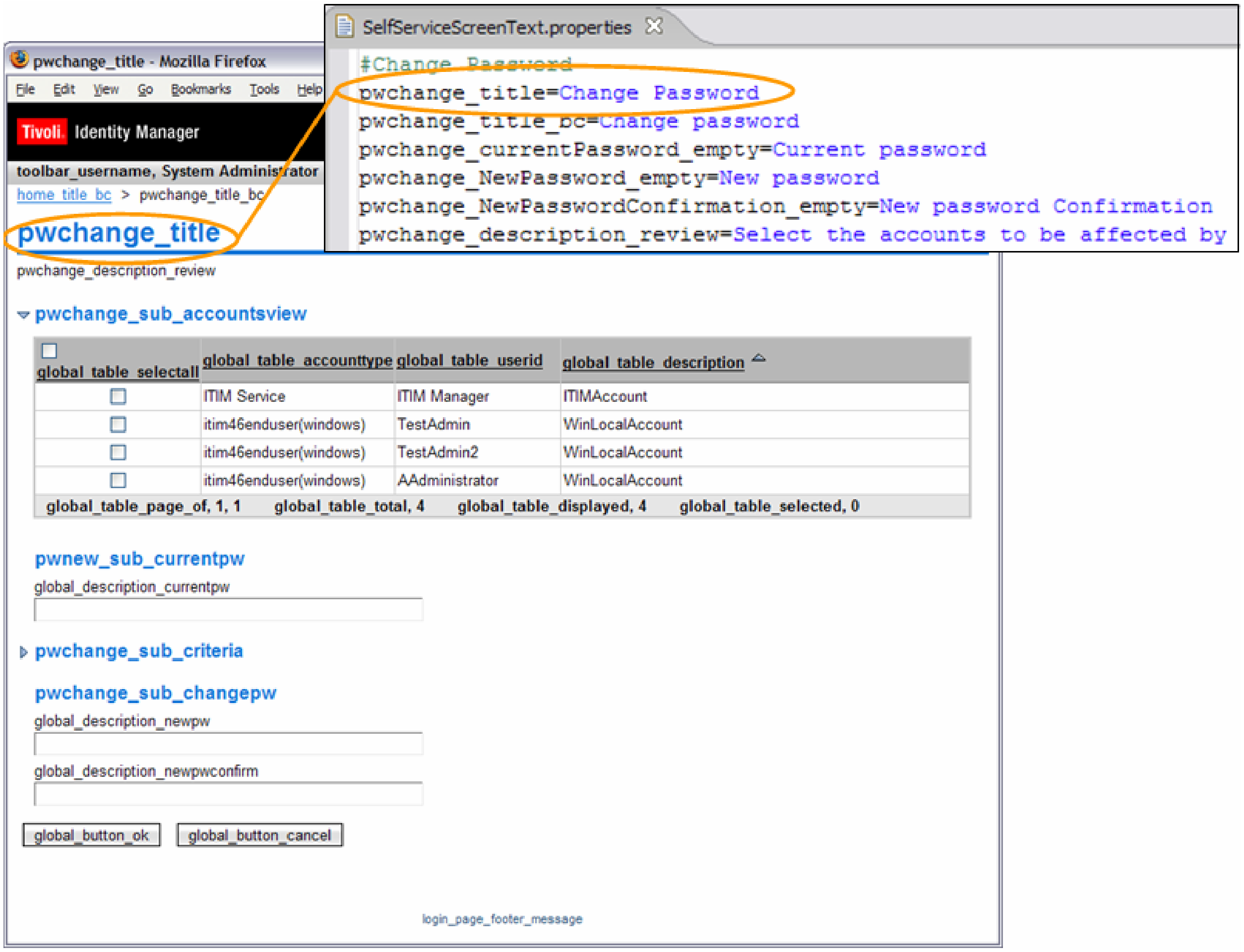
3. Restart the Self Service Application to make the change effective.

Determining the Key for a Screen Label

To help show the label keys for screen text an additional Resource Bundle, **SelfServiceScreenTextKeys.properties,** has been provided. This file contains all the screen text keys with the value of the label equal to the label key plus replacement parameters. This file can be used to display screen text label keys in the user interface. Figure 6: Label Keys Displayed shows an example of the Self Service user interface with the label keys displayed.

To use this file:

1. To preserve the current screen text, make a backup copy of the **SelfServiceScreenText.properties** file.
2. Copy the **SelfServiceScreenTextKeys.properties** file to **SelfServiceScreenText.properties**.
3. Restart the Self Service Application.


SelfServiceScreenText.properties
pwchange_title - Mozilla Firefox
File
Edit
View
Go
Bookmarks
Tools
Help
Tivoli. Identity Manager
toolbar_username, System Administrator
home_title_bc > pwchange_title_bc
pwchange_title
pwchange_description_review
pwchange_sub_accountsview
pwnew_sub_currentpw
global_description_currentpw
pwchange_sub_criteria
pwchange_sub_changepw
global_description_newpw
global_description_newpwconfirm
global_button_ok
global_button_cancel
login_page_footer_message

```
#Change Password
pwchange_title=Change Password
pwchange_title_bc=Change password
pwchange_currentPassword_empty=Current password
pwchange_NewPassword_empty=New password
pwchange_NewPasswordConfirmation_empty=New password Confirmation
pwchange_description_review=Select the accounts to be affected by
```

☐ global_table_selectall	global_table_accounttype	global_table_userid	global_table_description
☐	ITIM Service	ITIM Manager	ITIMAccount
☐	itim46enduser(windows)	TestAdmin	WinLocalAccount
☐	itim46enduser(windows)	TestAdmin2	WinLocalAccount
☐	itim46enduser(windows)	AAdministrator	WinLocalAccount

global_table_page_of, 1, 1   global_table_total, 4   global_table_displayed, 4   global_table_selected, 0

Figure 6: Label Keys Displayed

Person and Account Form Labels

The person and account forms displayed in the Self Service application are based on the Identity Manager 4.6 Form Customization feature. The labels for the form fields are stored in the **<ITIM_HOME>\data\CustomLabels.properties** file. The label for a field on a form can be determined using the Form Designer Applet using the following steps:

1. Log into the Identity Manager console as an administrator (http://<hostname>/enrole/logon).

2. Navigate to **“Configuration” → “Form Customization”**

3. Select the form and attribute you would like to change the text for.

4. Under **“Properties”→ “Form”** edit the **“Label”** attribute

    a. If the label starts with a $ then it will be looked up using the **CustomLabels.properties** resource bundle.

5. Save the changes to the form and/or update **CustomLabels.properties**.

If the label starts with a $ and its value was changed in **CustomLabels.properties**, the Self Service Application will have to be restarted for the change to take effect.

If the modified label does not start with a $ (i.e. no lookup in **CustomLabels.properties** is performed), then the application restart is not needed.

Text that cannot be replaced

Although the majority of the text in the Self Service application can be customized there are a few exceptions.

1. Error messages: Error message text is not available for editing/customization

2. Help content: The text in help content (reached by clicking the help link) is not editable. However, it is possible to redirect help requests to a different URL completely. See section Redirecting Help Content.

Customizing Banner, Footer, Navigation Bar, and Tool Bar

Two options are provided for configuring main layout elements of the Self Service application.

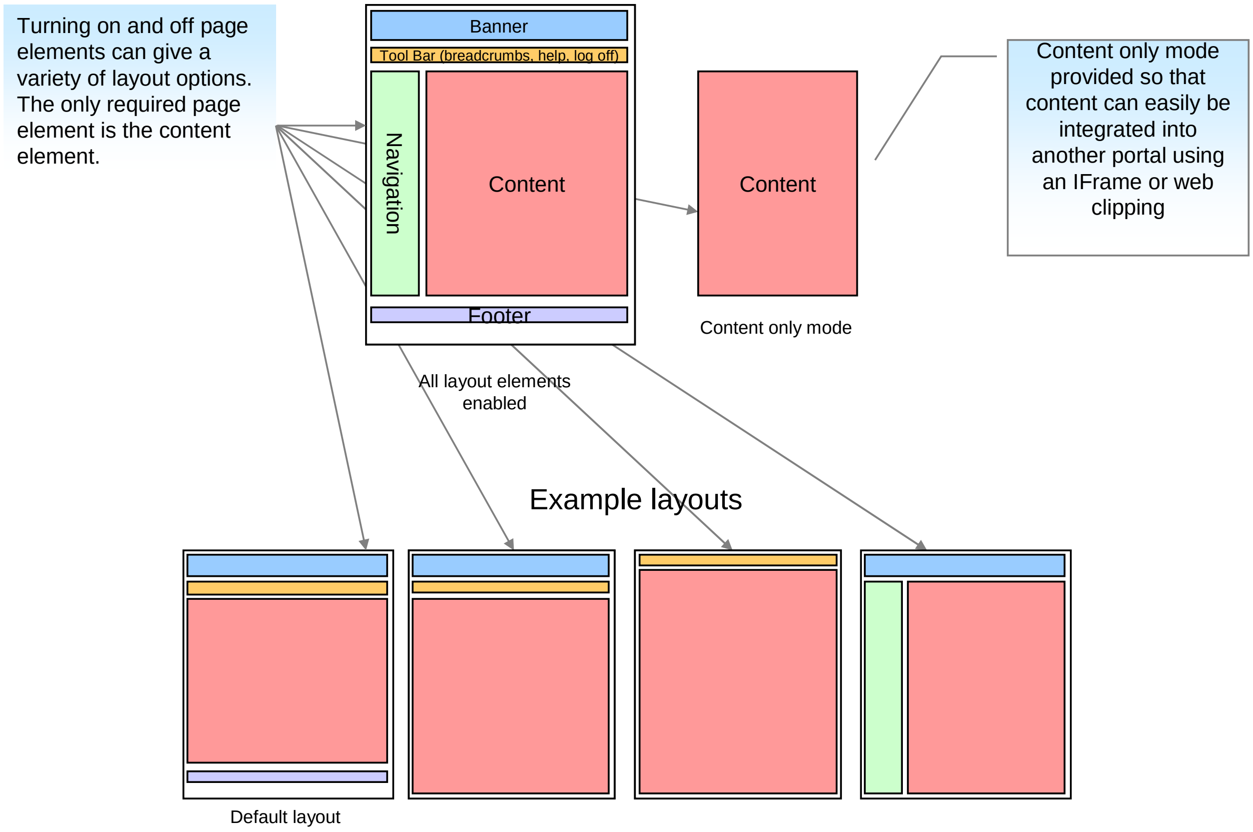
- Add / Remove the Banner, Footer, Navigation Bar, and Tool Bar from the page

- Replace the content of the Banner, Footer, Navigation Bar and Tool Bar for the page

Changing Layout

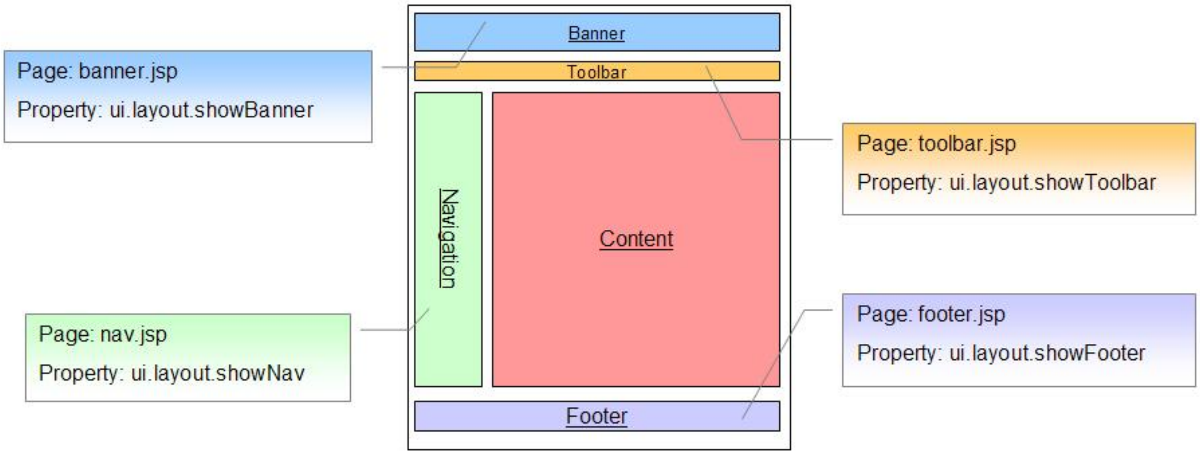
High level layout elements can be enabled / disabled from display on the Self Service user interface via settings in the **SelfServiceUI.properties** file. The default layout contains the Banner, Toolbar, and Footer.

Layout options


Turning on and off page elements can give a variety of layout options. The only required page element is the content element.

Content only mode provided so that content can easily be integrated into another portal using an IFrame or web clipping

Configuring Layout Elements in SelfServiceUI.properties


Page: banner.jsp
Property: ui.layout.showBanner

Page: toolbar.jsp
Property: ui.layout.showToolbar

Page: nav.jsp
Property: ui.layout.showNav

Page: footer.jsp
Property: ui.layout.showFooter

To show/hide a page element, change the ui.layout.show<name> property in **SelfServiceUI.properties** file. Setting a property to ‘true’, indicates the element should be included in the page; ‘false’ indicates that the element should not be included in the page.

Property	**Details**
ui.layout.showBanner	Controls the banner section. The default banner contains IBM / Product images.
ui.layout.showFooter	Controls the footer section. The default footer contains the product copyright.
ui.layout.showToolbar	Controls the toolbar section. The default toolbar contains the welcome message, help link, logoff link, and bread crumbs.
ui.layout.showNav	Controls the Navigation bar. **Note:** No default content is included for the navigation bar.

Any change to the **SelfServiceUI.properties** file requires a restart of the Self Service Application in WebSphere to make the change effective.

Replacing Banner, Footer, Navigation Bar, and Tool Bar content

Content in the **itim_self_service.war/custom/** directory can be replaced or modified to alter the look and feel of the Self Service application. This includes replacing or modifying the layout elements described above.

File names and content

The layout elements are JSP fragments that will be included in the layout of the webpage when the JSP is rendered. To modify these files

1. Copy the files from the deployed WebSphere directory, **<WAS_HOME>/installedApps/<cellName>/ITIM_Self_Service.ear/itim_self_service.war/custom/** to a temporary directory.
2. Edit the files and copy the updated files back into the deployed WebSphere directory.

NOTE: the default versions of these files are shipped with the product archive. When applying Fix packs or interim fixes, the product archive will overlay customized files with default versions. Be sure to back up the custom version of the files you have created so your customizations are not lost.

Layout element	**File Name**
Banner	itim_self_service.war/custom/banner.jsp
Footer	itim_self_service.war/custom/footer.jsp
Navigation Bar	itim_self_service.war/custom/nav.jsp
Tool bar	itim_self_service.war/custom/toolbar.jsp

Request Properties for use in Custom Content

To support dynamic content such as bread crumbs, help links and user IDs, a few request parameters have been made available including:

Property Name	Value	Description
loggedIn	***true*** or ***false***	Flag indicating if the user is currently logged in.
usercn	Common Name of the owner of the logged in account	**Note** this value is only set if the user is logged in.
langOrientation	***ltr*** or ***rtl***	Indicates the language direction of the current locale.
helpUrl	/itim/self/Help.do?helpId=home_help_url	URL to the help webpage with the helpId parameter set for the current page.
HelpLink	home_help_url	The helpId for the current page. Maps to the key in SelfServiceHelp.properties
breadcrumbs	Message keys for Breadcrumb text	Message key for breadcrumb text from SelfServiceScreenText.properties
breadcrumbLinks	Action path to build URL if bread crumb is linked	Action path to build URL if bread crumb is linked

Toolbar.jsp logic examples

The default “toolbar.jsp” contains the logic to display the welcome message and help links. This logic can be moved into the other layout elements; for example, the welcome message could be provided in the banner.

Displaying the Welcome Message

The code below checks to see if the user’s common name is set. If so, it translates the Welcome message substituting the name into the message. **NOTE:** the ITIM Self Service message labels and keys are defined in the **SelfServiceScreenText,properties** file.

```
<%-- If the Users Common Name is not empty display it. Note this value is not
     set until the user is logged in --%>

<c:if test=”${!empty usercn}”>
    <%--Translate the Welcome, Common Name message passing in the name --%>
    <fmt:message key=”toolbar_username” >
        <fmt:param><c:out value=”${usercn}”/></fmt:param>
    </fmt:message>
</c:if>
```

Displaying Help Links

The following code adds the Help link to the page. The helpUrl is retrieved from help attributes, and the help label is translated for display.

```
<%-- Add Help Link to the page --%>

<a id=”helpLink” href=”javascript:launchHelp(‘<c:out value=’${helpUrl}’)”>
      <fmt:message key=”toolbar_help”/></a>
```

Supporting Logoff

The Logoff link should only be displayed if the user is currently logged in. The code below tests to see if the **loggedIn** request parameter is true and if so translates the label for the logoff link and includes the link in the page.

```
<%-- If the user is logged in display the logoff link --%>

<c:if test=”${loggedIn == true}”>
    <a id=”logofflink” href=”/itim/self/Login/Logoff.do”>
        <fmt:message key=”toolbar_logoff”/></a>
</c:if>
```

Displaying Breadcrumbs

The following code adds the breadcrumbs to the page. The **“breadcrumbs”** attribute contains the list of label keys for the breadcrumbs. The **breadcrumbLinks** contain URL information for each breadcrumb label. A value of *null* or empty for the **breadcrumbLinks** indicates that the breadcrumb should not be linkable.

```
<%-- If the breadcrumbs label keys are not empty then display --%>

<c:if test=”${!empty breadcrumbs}”>

    <c:forEach items=”${breadcrumbs}” var=”breadcrumb” varStatus=”status”>

        <c:if test=”${status.index > 0}”>
            &nbsp;&gt;&nbsp;
        </c:if>

        <c:choose>
            <%-- If the action link is not empty for the current label then
                 create a link for the breadcrumb --%>
            <c:when test=”${!empty breadcrumbLinks{status.index}}”>
                <html:link action=”${breadcrumbLinks{status.index}}”>
                <fmt:message key=”${breadcrumb}”/></html:link>
            </c:when>
            <%-- If the action link is empty then just translate the
                 label for the breadcrumb --%>
            <c:otherwise>
                <fmt:message key=”${breadcrumb}”/>
            </c:otherwise>
        </c:choose>

    </c:forEach>

</c:if>
```

Customizing the Home Page

The Home Page refers to the page that gets loaded in the Content layout element after a user logs into the Self Service application. This page is one of the pages available for customization in the deployed WebSphere directory:

<WAS_HOME>/installedApps/<cellName>/ITIM_Self_Service.ear/itim_self_service.war/custom/

Customizing the Home Page is a two step process:

1. Edit the **SelfServiceHomePage.properties**
2. Edit the **Home.jsp**

File names and content

Step 1 involves editing the section and task definitions that are specified in the **SelfServiceHomePage.properties**.

These definitions tie defined views to tasks, and group tasks into sections. The section and task definitions are defined in a properties file in the **<ITIM_HOME>/data** directory.

Property file description	File Name
Home Page section and task definitions	SelfServiceHomePage.properties

Step 2 involves editing the layout of these sections and tasks in the **Home.jsp** for display.

The Home Page layout element is a JSP fragment that will be included in the layout of the webpage when the JSP is rendered. To modify this file:

1. Copy the file from the deployed WebSphere directory,

   <WAS_HOME>/installedApps/<cellName>/ITIM_Self_Service.ear/itim_self_service.war/custom/

   to a temporary directory.
2. Edit the file and copy the updated file back into the deployed WebSphere directory.

NOTE: the default versions of these files are shipped with the product archive. When applying Fix packs or interim fixes, the product archive will overlay customized files with default versions. Be sure to back up the custom version of the files you have created so your customizations are not lost.

Layout element	File Name
Home Page	Itim_self_service.war/custom/Home.jsp

Request Properties for use in Home Page

To support dynamic content such as sections, action-needed sections, tasks, a Java bean has been made available as a request parameter called **HomePageForm**. The Home Page java bean contains a handful of methods that can be used to access information about sections and tasks.

The following properties are available for the **HomePageForm** Java bean:

Property Name	**Value**	**Description**
Sections	List of Section Java beans	A list of sections the current user has been granted to view.
sectionToTaskMap	Map of sections to their corresponding tasks	A Map that links a given Section java bean to a Task Java bean.
actionNeededSection	Section Java bean, or null	A Section Java bean containing the pending actions for the current user. A null is used if no pending actions exist for the current user.

The following properties are available for the Section Java bean:

Property Name	**Value**	**Description**
titleKey	List of Section Java beans	A list of sections the current user has been granted to view.
iconUrl	Icon URL, or null	The URL path for the icon to be used for this section. A null is used to indicate that no icon should be used.
iconAltTextKey	Text key	Text key to be used as the alternate text for this section's icon.
tasks	List of Task Java beans	A list of tasks that can be displayed in this section

The following properties are available for the Task Java bean:

Property Name	**Value**	**Description**
urlPath	URL	A URL path to this task.
urlKey	Text key	The text key to be used for the link to this task.
descriptionKey	Text key	Text key to be used as the description of this task.

Obtaining the **HomePageForm** Java bean, iterating through the available sections and tasks and creating links to each available task:

```
<c:set var="pageConfig" value="${HomePageForm}" scope="page" />
<c:forEach items="${pageConfig.sections}" var="section">
      <%-- Process each section here --%>
      <c:forEach items="${pageConfig.sectionToTaskMap[section]}" var="task">
      <%-- Process each section here --%>
            <a href="/itim/self/<c:out value="${task.urlPath}"/>"
               title="<fmt:message key="${task.urlKey}" />">
```

```
                <fmt:message key="${task.urlKey}" />
            </a>
            <fmt:message key="${task.descriptionKey}" />
        </c:forEach>
</c:forEach>
```

Customizing Look and Feel using Style Sheets

Cascading Style Sheets (CSS) are used to style the look and feel of the user interface of the Self Service Application. The style sheet can be edited to modify the fonts, colors, and other styles associated with the Self Service Application. This section will discuss the location of the style sheet, and key styles to edit in order to customize the Self Service Application to match the look and feel of your company's website.

Style Sheet Details

Content in the CSS files in the **itim_self_service.war/custom/** directory can be replaced or modified to alter the look and feel of the Self Service application. This includes replacing or modifying the style sheets contained in the custom directory.

File names and content

To change the look and feel of the Self Service Application, take the following steps.

1. Copy the files from the deployed WebSphere directory, **<WAS_HOME>/installedApps/<cellName>/ITIM_Self_Service.ear/itim_self_service.war/custom/**

   to a temporary directory.
2. Edit the files and copy the updated files back into the deployed WebSphere directory.

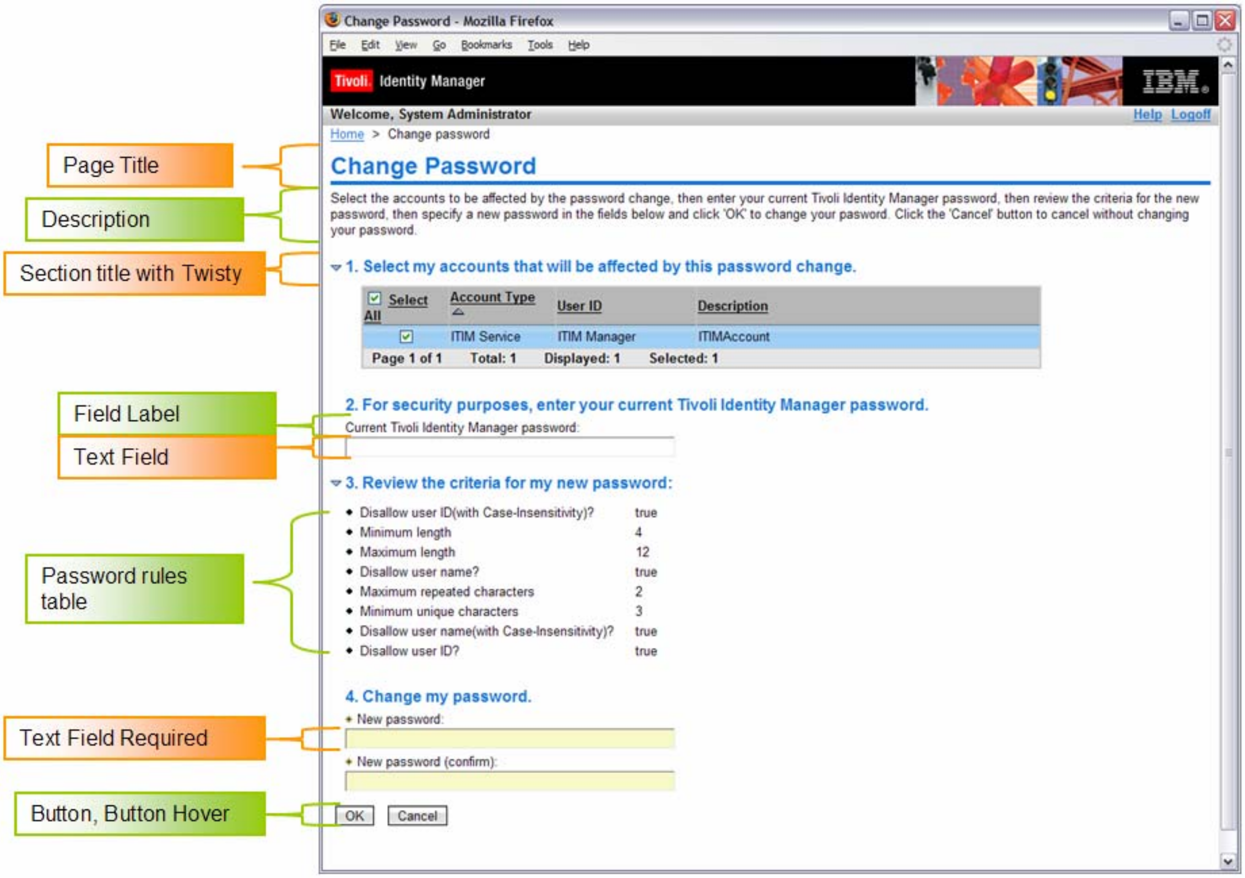
NOTE: the copy of the default version of these files is shipped with the product archive. When applying Fix packs or interim fixes, the product archive will overlay customized files with default versions. Be sure to back up the custom version of the files you have created so your customizations are not lost.

CSS file	File Description
end_user.css	CSS file containing main CSS styles for left to right language orientation
end_user_rtl.css	CSS file containing main CSS styles for right to left language orientation
widgets.css	CSS file containing styles used for widgets contained in Profile, Account, and RFI forms for left to right language orientation. **Note:** Editing this file takes more advanced CSS skills.

CSS file	File Description
widgets_rtl.css	CSS file containing styles used for widgets contained in Profile, Account, and RFI forms for right to left language orientation. **Note:** Editing this file takes more advanced CSS skills.
date_Widget_ltr.css	CSS file containing styles used for date widgets contained in Profile, Account, and RFI forms for left to right language orientation. **Note:** Editing this file takes more advanced CSS skills.
date_Widget_rtl.css	CSS file containing styles used for date widgets contained in Profile, Account, and RFI forms for right to left language orientation. **Note:** Editing this file takes more advanced CSS skills.
time.css	CSS file containing styles used for time widgets contained in Profile, Account, and RFI forms. **Note:** Editing this file takes more advanced CSS skills.
calendar.css	CSS file containing styles used for calendar widgets contained in Profile, Account, and RFI forms. **Note:** Editing this file takes more advanced CSS skills
customForm.css	CSS file containing styles used to layout forms used in Profile, Account and RFI forms for left to right language orientation. **Note:** Editing this file takes more advanced CSS skills.
customForms_rtl.css	CSS file containing styles used to layout forms used in Profile, Account and RFI forms for right to left language orientation. **Note:** Editing this file takes more advanced CSS skills.

Primary CSS Styles

This section will cover the main CSS styles in the user interface. The figures display different styles below.



Change Password

Select the accounts to be affected by the password change, then enter your current Tivoli Identity Manager password, then review the criteria for the new password, then specify a new password in the fields below and click 'OK' to change your pasword. Click the 'Cancel' button to cancel without changing your password.

1. Select my accounts that will be affected by this password change.

☑ Select All	Account Type	User ID	Description
☑	ITIM Service	ITIM Manager	ITIMAccount

Page 1 of 1 Total: 1 Displayed: 1 Selected: 1

2. For security purposes, enter your current Tivoli Identity Manager password.

Current Tivoli Identity Manager password:

3. Review the criteria for my new password:

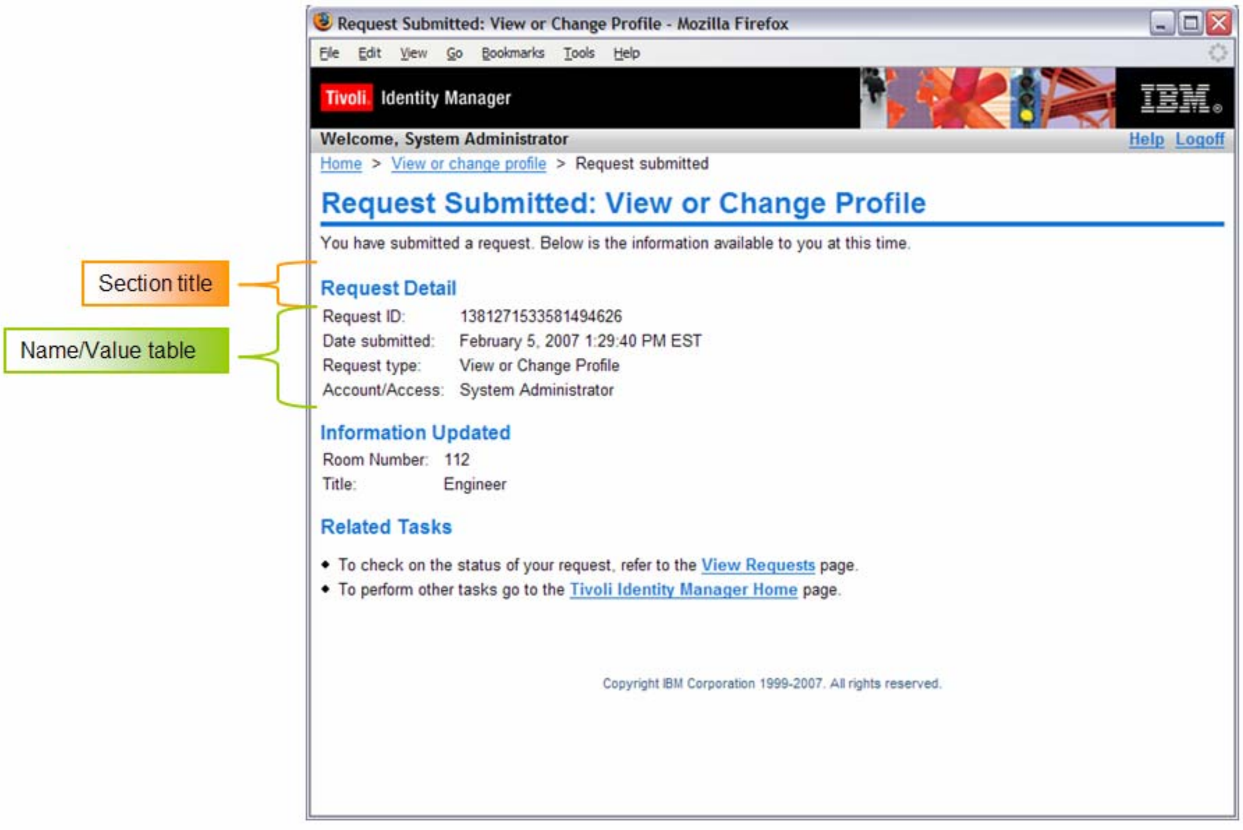
Disallow user ID(with Case-Insensitivity)?	true
Minimum length	4
Maximum length	12
Disallow user name?	true
Maximum repeated characters	2
Minimum unique characters	3
Disallow user name(with Case-Insensitivity)?	true
Disallow user ID?	true

4. Change my password.

* New password:

* New password (confirm):

Figure 7 Page Elements


Section title
Name/Value table
Request Submitted: View or Change Profile - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
Tivoli. Identity Manager
IBM.
Help Logoff

Welcome, System Administrator

Home > View or change profile > Request submitted

Request Submitted: View or Change Profile

You have submitted a request. Below is the information available to you at this time.

Request Detail

Request ID:	1381271533581494626
Date submitted:	February 5, 2007 1:29:40 PM EST
Request type:	View or Change Profile
Account/Access:	System Administrator

Information Updated

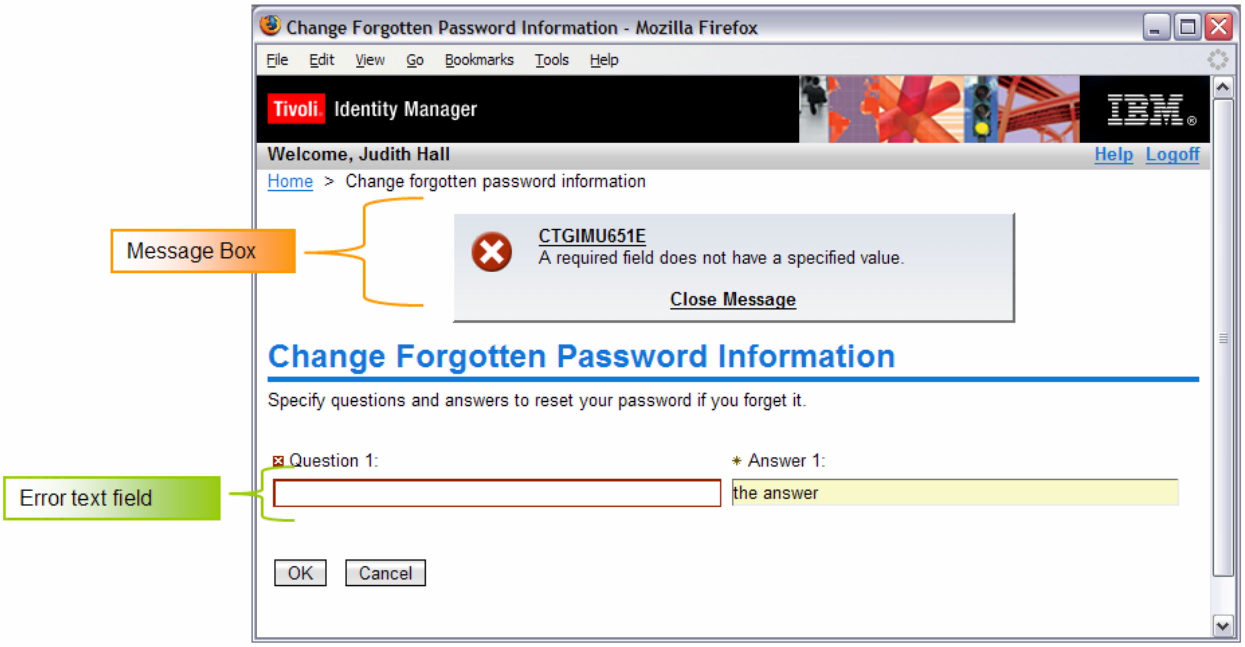
Room Number:	112
Title:	Engineer

Related Tasks

- To check on the status of your request, refer to the View Requests page.
- To perform other tasks go to the Tivoli Identity Manager Home page.

Copyright IBM Corporation 1999-2007. All rights reserved.

Figure 8: Page elements 2


Message Box
Error text field
Change Forgotten Password Information - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
Tivoli. Identity Manager
IBM.
Help Logoff
Close Message
OK
Cancel

Welcome, Judith Hall

Home > Change forgotten password information

CTGIMU651E
A required field does not have a specified value.

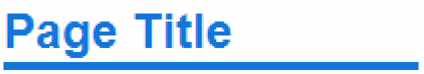
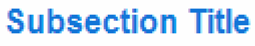
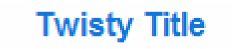
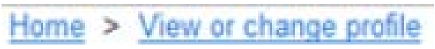
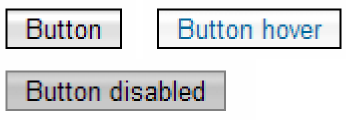
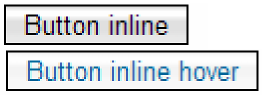
Change Forgotten Password Information

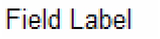
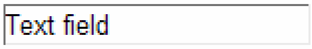
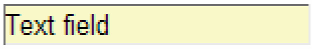
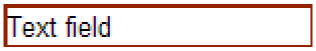
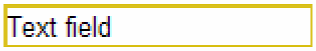
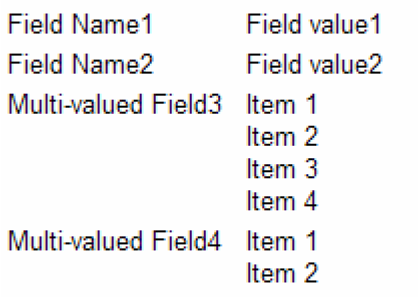
Specify questions and answers to reset your password if you forget it.

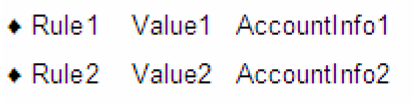
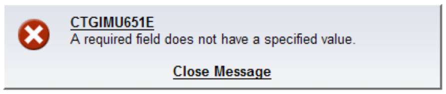
Question 1:	* Answer 1:
	the answer

Figure 9: Page elements 3

CSS Reference Table, Main Styles

Element	Example	Main Style Selector	Description
Page Title	 Page Title	Type selector: h1	All Page titles
Section Title	 Subsection Title	Type selector: h2	Section titles for page that do not contain a twisty
Section Titles with Twisties	 Twisty Title	Type selector: h3	Section titles on page which contains twisty sections. The titles are indented to allow space for the twisty image
Breadcrumbs	 Home > View or change profile	Type selector: #breadcrumbs	Breadcrumbs navigation trail shown top left above Page Title
Button, Button Hover, Disabled Button	 Button Button hover Button disabled	Class selectors: .button .button_hover .button_disabled	The button styles cover the majority of buttons in the UI. The hover style is used when a mouse hovers over the button
Inline button, Inline button hover	 Button inline Button inline hover	Class selectors: .button_inline .button_inline_hover	Used for a subset of buttons with special layout requirements
Page/Section descriptions	This is a description	Class selector: .description	Page and section descriptions. The description is contained in a <div> block. Therefore, you could add borders, colors etc. if desired.

Element	Example	Main Style Selector	Description
Field Labels	 Field Label	Type selector: label	Field labels on forms
Text field	 Text field	Class selector: input.textField_std	Standard text fields
Required text field	 Text field	Class selector: input.textField_required	Required text fields
Error text field	 Text field	Class selector: input.textField_error	Text fields in an error state
Warning text field	 Text field	Class selector: input.textField_warning	Text fields in a warning state
Field/Value Tables	 Field Name1 Field value1 Field Name2 Field value2 Multi-valued Field3 Item 1 Item 2 Item 3 Item 4 Multi-valued Field4 Item 1 Item 2	Type.Class selector table.nameValueTable	Field value tables are used through out the UI to display a field name and one or more corresponding values. For example, the Information section of the request submitted pages use name value tables. The selector is shown for the table. Additional selectors exist that style the rows, cells, multi value lists, and name column for this table.

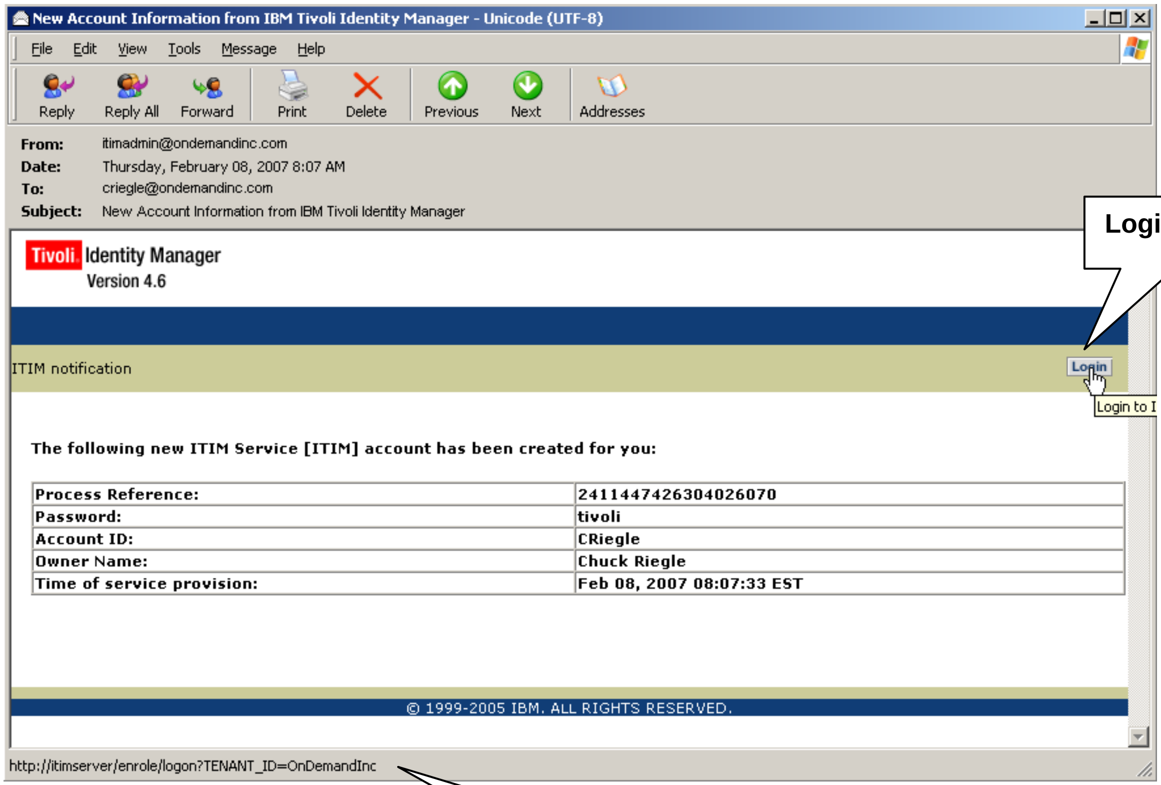
Element	Example	Main Style Selector	Description
Password rules Table	 ◆ Rule1 Value1 AccountInfo1 ◆ Rule2 Value2 AccountInfo2	Class selectors .pwRulesTable .pwRules .ruleCol .pwRules .valueCol .pwRules .accountInfoCol	The password rules table is used to style the password rules sections through out the UI. The table consists of three columns; a rule column, a value column and an account information column.
Message Box	 CTGIMU651E A required field does not have a specified value. Close Message	div.messageBoxComposite	The message box composite is the main CSS selector for the message box. Additional selectors exist to specify the image / link / and message layout.

Customizing Workflow Notification Templates

Tivoli Identity Manager 4.6 provides a comprehensive set of notification templates that are used to create emails to notify users about workflow activities (new account, new password, change account, deprovision account, suspend account, restore account, etc.).

The Workflow Notification Templates provide two formats for emails; text and XHTML. The HTML emails generated from these Tivoli Identity Manager Workflow notifications contain an HTML form with a **Login** button. When a user clicks the **Login** button, they are directed to the Tivoli Identity Manager user interface and not the ITIM Self Service Application User Interface.

Following is a sample account notification email. Note the url associated with the **Login** button action.


New Account Information from IBM Tivoli Identity Manager - Unicode (UTF-8)
File Edit View Tools Message Help
Reply
Reply All
Forward
Print
Delete
Previous
Next
Addresses
Tivoli Identity Manager
Version 4.6
Login
Login to I

From: itimadmin@ondemandinc.com
Date: Thursday, February 08, 2007 8:07 AM
To: criegle@ondemandinc.com
Subject: New Account Information from IBM Tivoli Identity Manager

ITIM notification

The following new ITIM Service [ITIM] account has been created for you:

Process Reference:	**2411447426304026070**
Password:	**tivoli**
Account ID:	**CRiegle**
Owner Name:	**Chuck Riegle**
Time of service provision:	**Feb 08, 2007 08:07:33 EST**

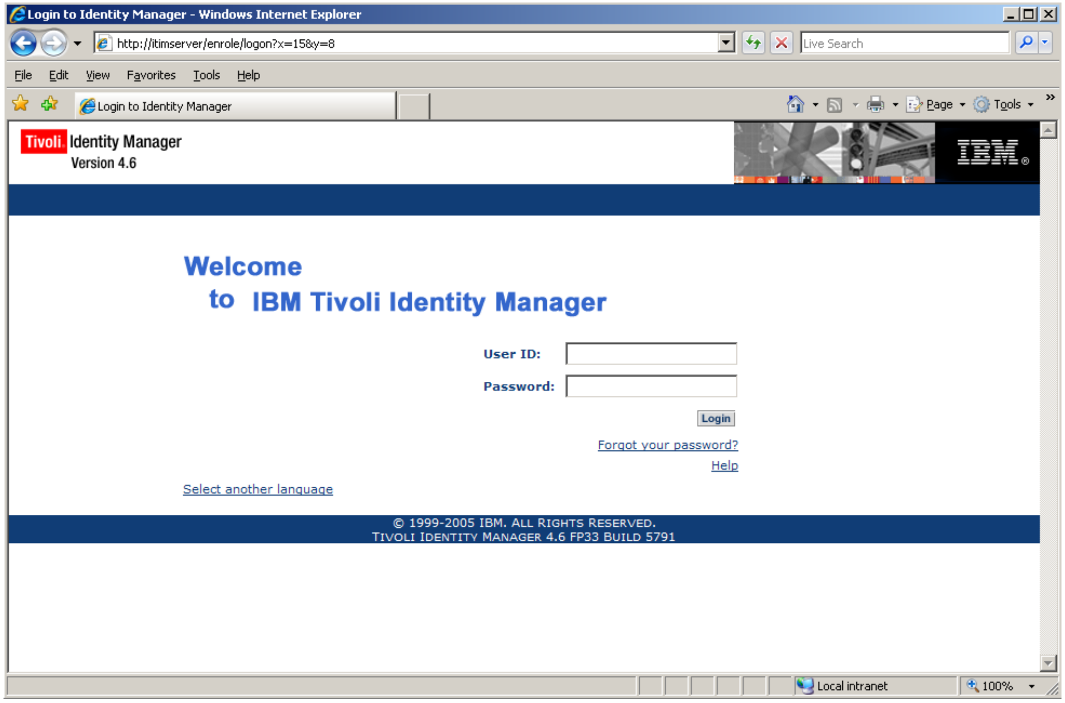
© 1999-2005 IBM. ALL RIGHTS RESERVED.

http://itimserver/enrole/logon?TENANT_ID=OnDemandInc

Login button

http://<hostname>/enrole/logon

Clicking on the **Login** button takes the user to the login page of the Tivoli Identity Manager User Interface.



Welcome to IBM Tivoli Identity Manager

© 1999-2005 IBM. ALL RIGHTS RESERVED.
TIVOLI IDENTITY MANAGER 4.6 FP33 BUILD 5791

The action associated with the **Login** button in the email templates can be changed to send the user to the ITIM Self Service Application. The button action can direct users to the login page or it can be used to direct users to specific pages such as 'View Account' or 'Approve and Review Requests'.

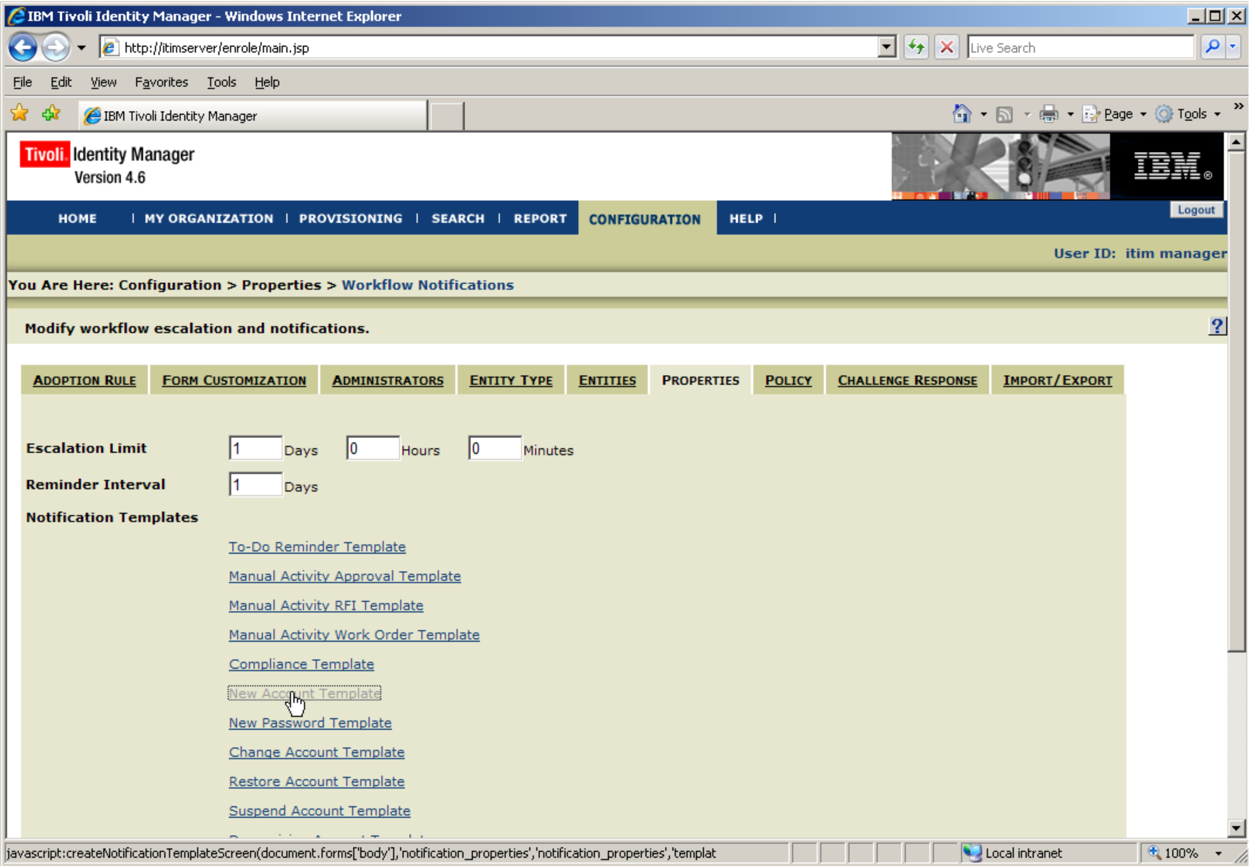
There are several base Workflow Notification templates which are used during Workflow Notification Activities. Administrators will have to change the **Login** button action on each template. If the administrator has modified the Workflow Notification Templates in any Workflows (including custom workflows that have been created), they will also have to change the Notification Templates in those Workflows.

The following Workflow Notifications have templates which send emails containing HTML forms with the **Login** button:

- New account
- New password
- Change account
- Deprovision account
- Suspend account
- Restore account
- Manual Activity Approval
- Manual Activity Request for Information
- Compliance Alert
- Activity Timeout
- Process Timeout
- Process Completion

The default **Login** button takes users to the login page of the Tivoli Identity Manager user interface. The following steps demonstrate how to change the base Workflow Notification Templates so users are directed to the login page of the ITIM Self Service user interface:

1. Login to the Tivoli Identity Manager User Interface with a user which has Administrative authority.
2. Click on the **CONFIGURATION** tab.
3. Click on the **<u>PROPERTIES</u>** tab.
4. Click on the Workflow Notification control **[…]**
5. Click on a Notification Template that you wish to change (eg. <u>New Account Template</u>)


IBM Tivoli Identity Manager - Windows Internet Explorer
http://itimserver/enrole/main.jsp
Live Search
File Edit View Favorites Tools Help
IBM Tivoli Identity Manager
Page Tools
Tivoli Identity Manager
Version 4.6
IBM
HOME | MY ORGANIZATION | PROVISIONING | SEARCH | REPORT CONFIGURATION HELP |
Logout
User ID: itim manager
You Are Here: Configuration > Properties > Workflow Notifications
Modify workflow escalation and notifications.
?
ADOPTION RULE
FORM CUSTOMIZATION
ADMINISTRATORS
ENTITY TYPE
ENTITIES
PROPERTIES
POLICY
CHALLENGE RESPONSE
IMPORT/EXPORT
Notification Templates
To-Do Reminder Template
Manual Activity Approval Template
Manual Activity RFI Template
Manual Activity Work Order Template
Compliance Template
New Account Template
New Password Template
Change Account Template
Restore Account Template
Suspend Account Template
Local intranet
100%

Escalation Limit 1 Days 0 Hours 0 Minutes

Reminder Interval 1 Days

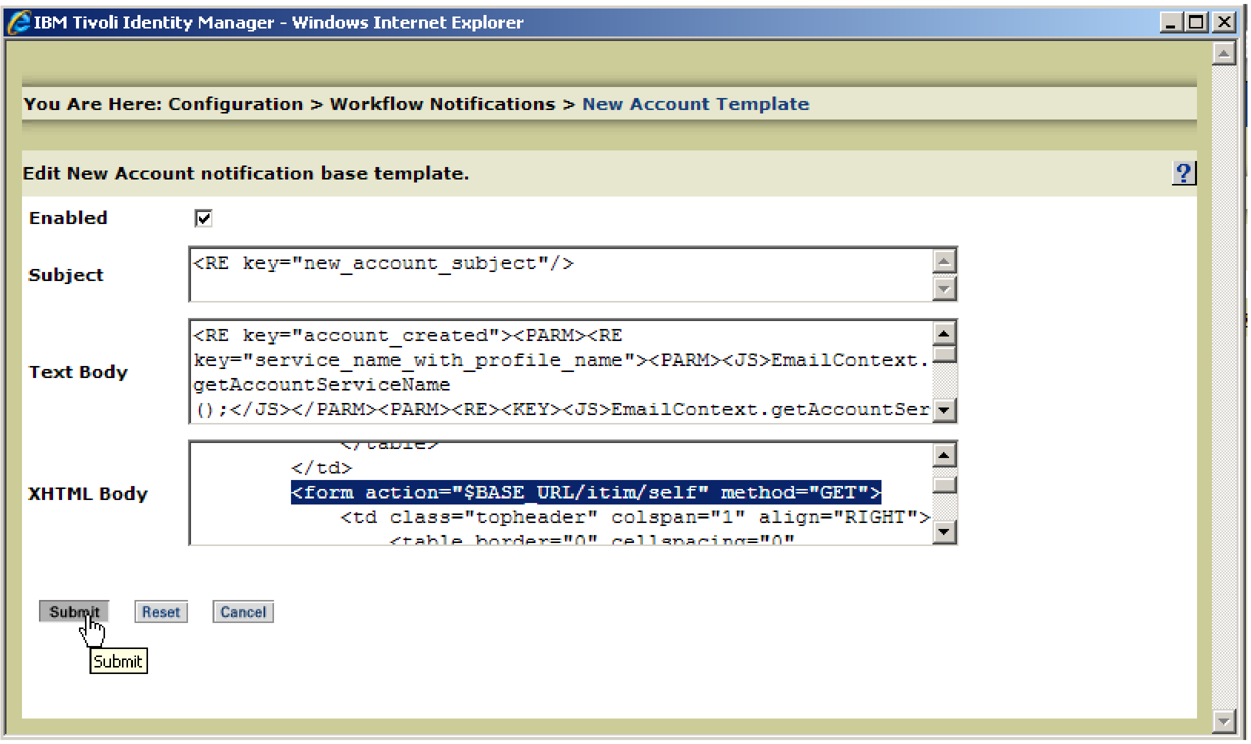
javascript:createNotificationTemplateScreen(document.forms['body'],'notification_properties','notification_properties','templat

6. Scroll down in the **XHTML Body** edit box and look for the statement:

   <form action="$BASE_URL/**enrole/logon$TENANT_ID**" method="GET">

7. Change the text **enrole/logon$TENANT_ID** to **itim/self**. The new statement should look like this:

   <form action="$BASE_URL/**itim/self**" method="GET">



You Are Here: Configuration > Workflow Notifications > New Account Template

Edit New Account notification base template.

Enabled ☑

Subject

```
<RE key="new_account_subject"/>
```

Text Body

```
<RE key="account_created"><PARM><RE
key="service_name_with_profile_name"><PARM><JS>EmailContext.
getAccountServiceName
();</JS></PARM><PARM><RE><KEY><JS>EmailContext.getAccountSer
```

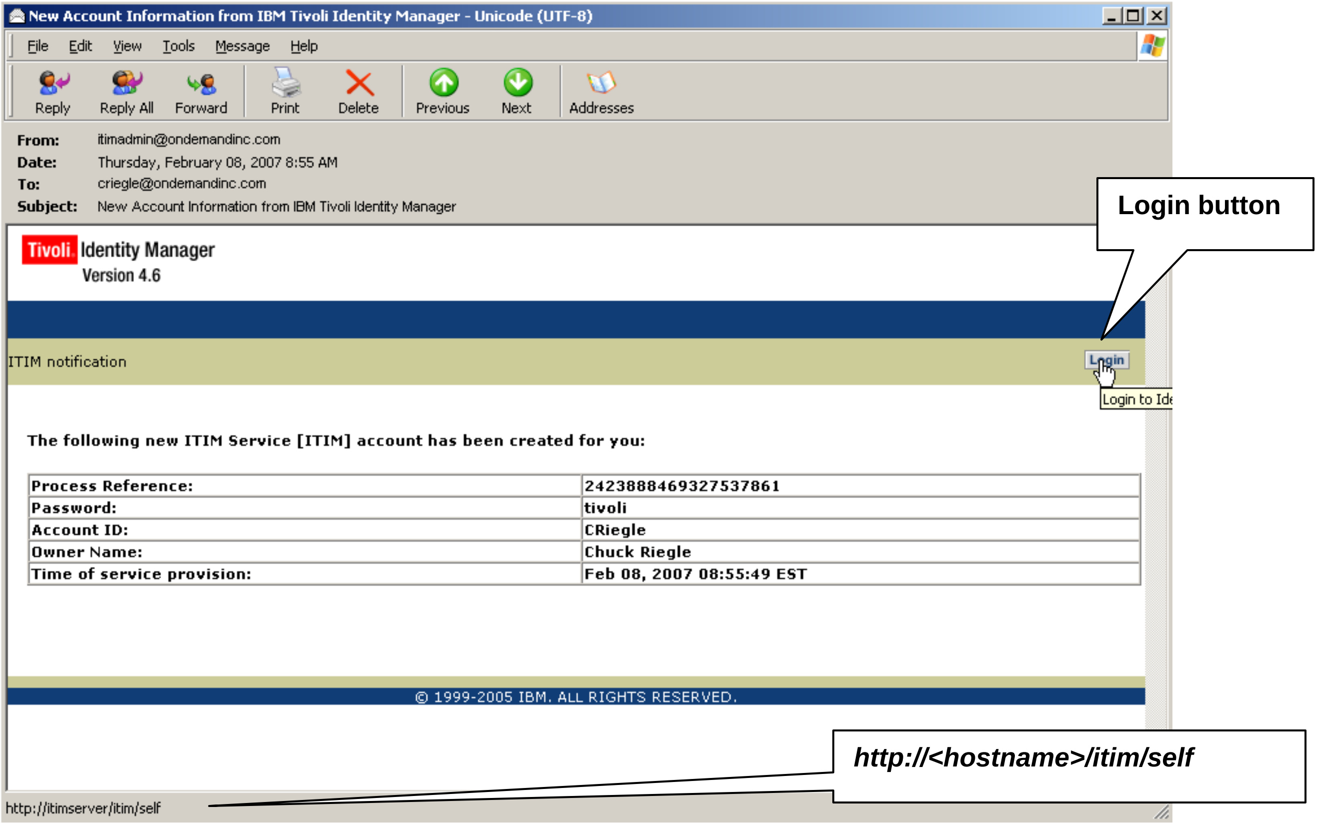
XHTML Body

```
          </table>
        </td>
        <form action="$BASE_URL/itim/self" method="GET">
            <td class="topheader" colspan="1" align="RIGHT">
                <table border="0" cellspacing="0"
```

8. Click on the **Submit** button.

9. Click on the **Done** button.

The action associated with the **Login** button in the email notification is changed.


New Account Information from IBM Tivoli Identity Manager - Unicode (UTF-8)
File Edit View Tools Message Help
Reply
Reply All
Forward
Print
Delete
Previous
Next
Addresses
Login
Login to Ide

From: itimadmin@ondemandinc.com
Date: Thursday, February 08, 2007 8:55 AM
To: criegle@ondemandinc.com
Subject: New Account Information from IBM Tivoli Identity Manager

Tivoli. Identity Manager
Version 4.6

ITIM notification

The following new ITIM Service [ITIM] account has been created for you:

Process Reference:	**2423888469327537861**
Password:	**tivoli**
Account ID:	**CRiegle**
Owner Name:	**Chuck Riegle**
Time of service provision:	**Feb 08, 2007 08:55:49 EST**

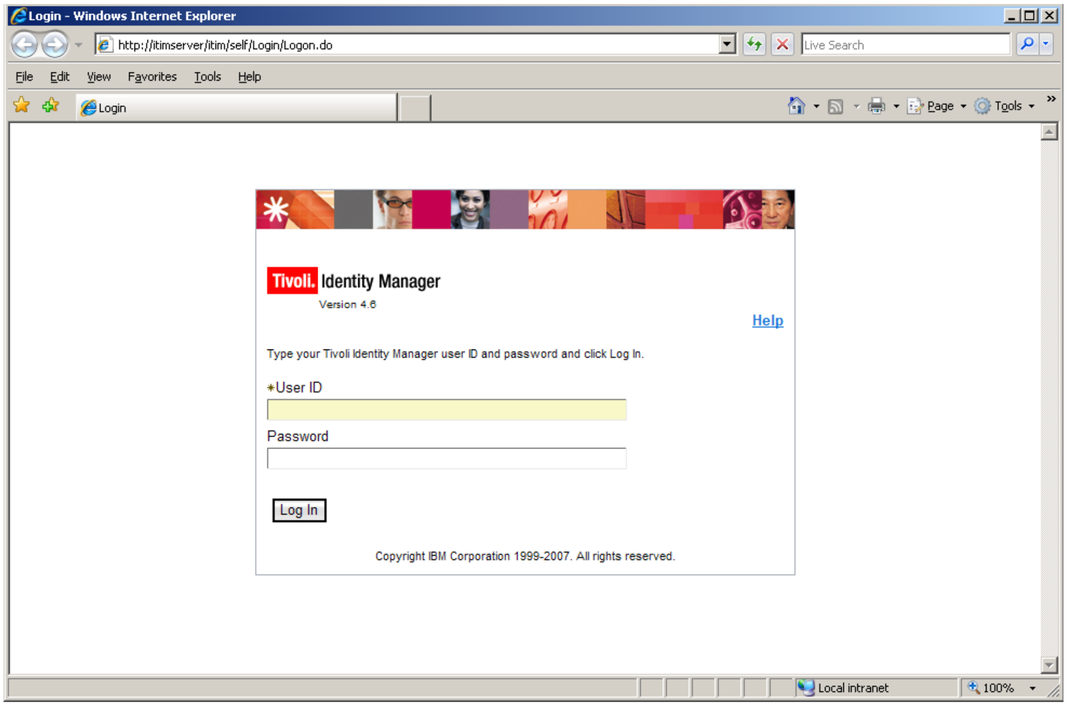
© 1999-2005 IBM. ALL RIGHTS RESERVED.

http://itimserver/itim/self

Login button

http://<hostname>/itim/self

Clicking on the **Login** button in the New Account Notification email will now direct the user to the login page of the ITIM Self Service user interface.


Login - Windows Internet Explorer
http://itimserver/itim/self/Login/Logon.do
Live Search
File Edit View Favorites Tools Help
Login
Page
Tools
Local intranet
100%

Tivoli. Identity Manager
Version 4.6

Help

Type your Tivoli Identity Manager user ID and password and click Log In.

*User ID

Password

Log In

Copyright IBM Corporation 1999-2007. All rights reserved.

To direct users to pages other than the login page of the Self Service user interface, change the form action associated with the **Login** button provided in the email template. The following table provides a few examples:

Self Service UI Page	Email Template Form Action
Login page	<form action="$BASE_URL/**itim/self**" method="GET">
View/Change Accounts	<form action="$BASE_URL/**itim/self/ChangeAccount.do**" method="GET"
Review Activities	<form action="$BASE_URL/**itim/self/ReviewActivities.do**" method="GET">

Redirecting Help Content

Editing the out-of-the box help content shipped with the Self Service application is not supported. But it is possible to redirect the help requests to your own website in order to deliver custom help content.

Editing SelfServiceHelp.properties

SelfServiceHelp.properties allows you to specify the base URL that Help requests will be sent to.

Property	Description
helpBaseUrl	Specifies the base url to send help requests to. A blank value indicates that help should go to the url for Self Service application help.
Help Id mappings: helpId = relative page URL	The help mappings section maps ids from specific pages to a relative URL sent to the help server.

How the help URL is constructed

The Help URL is the combination of helpBaseUrl + locale + relativeHelppageURL

For example:

helpBaseUrl=http://myserver:80
locale = en_US
loginId/relativeURL = login_help_url=ui/ui_eui_login.html
Final URL = http://myserver:80/en_US/ui/ui_eui_login.html

Locale is determined by resolving the **SelfServiceScreenText.properties** resource bundle for the current logged in user and using the associated locale.

Steps to Redirecting Help

1. Change helpBaseUrl in SelfServiceHelp.properties
2. Update helpId mappings to use the relative urls for your server
3. Add pages to your server for the appropriate locales
4. Restart the Self Service application.

6

Configuring Single Sign-On

Single Sign-On services provide a seamless experience for a user accessing a number of applications in the enterprise. This chapter provides the details to enable Single Sign-On for the Tivoli Identity Manager Self Service user interface using IBM Tivoli Access Manager.

With the Single Sign-On function configured, a user logs in once to IBM Tivoli Access Manager web security and the user's identity is propagated to Tivoli Identity Manager eliminating the need for another login.

This function requires Tivoli Access Manager to enable single sign-on capability with Tivoli Identity Manager.

1. Tivoli Access Manager performs user authentication and coarse-grained authorization before access is allowed to Tivoli Identity Manager.

2. Tivoli Identity Manager then applies fine-grained access control using its own Access Control Item (ACI).

There are two way to configure Tivoli Access Manger and Tivoli Identity Manager for Single Sign-On.

- Using WebSEAL

- Using Tivoli Access Manager Plug-in Servers

This document will cover how to configure Single Sign-On using WebSEAL to Tivoli Identity Manager using the Tivoli Identity Manager Self Service application.

Before Configuring Single Sign-On with WebSEAL, ensure that Tivoli Access Manager and WebSEAL are installed and configured.

Configuring Single Sign-On with WebSEAL

Using WebSEAL authentication in place of Tivoli Identity Manager authentication eliminates the need for a separate password to access Tivoli Identity Manager using the ITIM Self Service application. The login to WebSEAL can use any authentication mechanism. The ITIM Self Service application logon panel does not appear during the Single Sign-On operation.

WebSEAL supports both standard TCP (HTTP) and secure SSL (HTTPS) junctions between WebSEAL and the Tivoli Identity Manager Server.

To Configure Single Sign-On with WebSEAL you must perform the following steps:

1. Define how Tivoli Identity Manager maps Tivoli Access Manager accounts to Tivoli Identity Manager accounts during authentication.

2. Define Tivoli Access Manager User accounts for the users that will need access to the ITIM Self Service Application.

3. Define a Tivoli Access Manager Group.

4. Add the Tivoli Access Manager users that require access to the ITIM Self Service Application to the Tivoli Access Manager Group.
5. Define a WebSEAL Junction.
6. Define a Tivoli Access Manager ACL to control access to the ITIM Self Service Application.
7. Grant the Tivoli Access Manager Group the appropriate access to the Tivoli Access Manager ACL.
8. Associate the WebSEAL junction to the Tivoli Access Manager ACL.
9. Configure Tivoli Identity Manager to use Single Sign-On.

TAM-ITIM Account Mapping

Using Single Sign-On, there is account mapping that occurs between Tivoli Access Manager and Tivoli Identity Manager during login authentication.

When a user logs into the ITIM Self Service application using WebSEAL and Single Sign-On, the user must specify a Tivoli Access Manager user account and password. Tivoli Access Manager performs user authentication and also checks to see if the user has been authorized to access the ITIM Self Service application. If the authentication and authorization are successful the Tivoli Access Manager user account is passed in the "**iv-user**" HTTP request header to the ITIM Self Service application. The ITIM Self Service application passes the information in the HTTP request header to Tivoli Identity Manager for further processing. Tivoli Identity Manager uses the Tivoli Access Manager user account to find a "matching" Tivoli Identity Manager user account in the Tivoli Identity Manager directory.

Usually the Tivoli Access Manager user account and Tivoli Identity Manager user account are identical. If they are identical, Tivoli Identity Manager will allow the user to login to the ITIM Self Service application. If they are not identical, you can configure Tivoli Identity Manager to perform user account mapping. There are two mapping configuration options available which are controlled by the **enrole.authentication.idsEqual** attribute in the **enRoleAuthentication.properties** file located in the ***ITIM_HOME***/data directory.

1. **enrole.authentication.idsEqual**=**true**

   No mapping is attempted. The Tivoli Access Manager user account passed in the "**iv-user**" HTTP request header must be identical to a Tivoli Identity Manager user account defined in the Tivoli Identity Manager directory in order for the user to be allowed to login to the ITIM Self Service application.

2. **enrole.authentication.idsEqual**=**false**

   The Tivoli Access Manager user account passed in the "**iv-user**" HTTP request header is used to search the Tivoli Identity Manager directory for a matching Tivoli Identity Manager user account:

   - If an identical Tivoli Identity Manager user account is found then the user is allowed to login to the ITIM Self Service application.

- If an identical Tivoli Identity Manager account is not found then Tivoli Identity Manager attempts to locate a “matching” Tivoli Identity Manager user account using the mapping logic below:

  The Tivoli Access Manager user account passed in the “**iv-user**” HTTP request header is used to search the Tivoli Identity Manager directory for a Tivoli Access Manager user account.

  If an identical Tivoli Access Manager user account is found in the Tivoli Identity Manager directory then a search is performed for the Tivoli Identity Person that owns the Tivoli Access Manager user account. If an owning Tivoli Identity Manager Person cannot be located the user is not allowed to login.

  If the Tivoli Identity Manager Person that owns the matching Tivoli Access Manager user account is found then a search is performed for a Tivoli Identity Manager user account owned by that Tivoli Identity Manager Person. If a Tivoli Identity Manager user account owned by the Tivoli Identity Manager Person is found then the user is allowed to login to the ITIM Self Service application using that Tivoli Identity Manager user account. Otherwise the user is not allowed to login.

Note: If the policy in your installation is that all Tivoli Identity Manager user accounts must have matching Tivoli Access Manager user accounts then you should specify **enrole.authentication.idsEqual=true** to avoid the unnecessary mapping processing and overhead.

Define TAM User Accounts

For those users that will need to access the ITIM Self Service Application you will need to define Tivoli Access Manager user accounts in addition to Tivoli Identity Manager user accounts. It is recommended that their Tivoli Access Manager user account and Tivoli Identity Manager user account are identical otherwise you must configure the user account mapping in the previous section.

To simplify the examples in this section the Tivoli Access Manager **pdadmin** command utility will be used to define Tivoli Access Manager user accounts. You could also use the Tivoli Access Manager Web Portal Manager GUI or Tivoli Identity Manager. It is recommended that you use Tivoli Identity Manager to provision the Tivoli Access Manager user accounts.

You must run the **pdadmin** command utility from a machine where the Tivoli Access Manager Runtime is installed. This may be on the Tivoli Access Manager Authorization Server or the Tivoli Access Manager Policy Server.

To start the Tivoli Access Manager **pdadmin** utility, enter **pdadmin** at a command prompt.

Login to a secure domain as the **sec_master** administration user to use the utility. At the **pdadmin>** command prompt, type **login**. Type **sec_master** at the **Enter User ID:** prompt. Specify the associated password at the **Enter Password** prompt.

For example:

```
pdadmin> login
Enter User ID: sec_master
Enter Password: password
pdadmin>
```

In the example below the Tivoli Access Manager user account **gforghetti** will be defined. This same user account has also been defined as a Tivoli Identity Manager user account.

To define the Tivoli Access Manager user account **gforghetti** using the **pdadmin** command utility enter the following command (on 1 complete line) from the **pdadmin>** command prompt:

```
user create "gforghetti" "cn=Gary Forghetti,o=ibm,c=us" "Gary Forghetti"
"Forghetti" password
```

where ***password*** is the user's password.

To make the user account valid enter the following command:

```
user modify "gforghetti" account-valid yes
```

Define a TAM Group

To simplify the example in this section the Tivoli Access Manager **pdadmin** command utility will be used to define Tivoli Access Manager Groups. You could also use the Tivoli Access Manager Web Portal Manager GUI.

Assuming you are already logged in to the **pdadmin** command utility, enter the following command (on 1 complete line) from the **pdadmin>** command prompt to create the Group **ITIM-Self-Service-Group**:

```
group create ITIM-Self-Service-Group cn=ITIM-Self-Service-Group,o=ibm,c=us
ITIM-Self-Service-Group
```

Add TAM User Accounts to the TAM Group

To simplify the example in this section the Tivoli Access Manager **pdadmin** command utility will be used to add the Tivoli Access Manager user accounts to the Tivoli Access Manager Groups. You could also use the Tivoli Access Manager Web Portal Manager GUI or Tivoli Identity Manager. It is recommended that you use Tivoli Identity Manager to perform that provisioning.

Assuming you are already logged in to the **pdadmin** command utility, enter the following command from the **pdadmin>** command prompt to add the Tivoli Access Manager user account gforghetti to the Group **ITIM-Self-Service-Group**:

```
group modify ITIM-Self-Service-Group add "gforghetti"
```

Defining a WebSEAL SSL Junction

Defining a WebSEAL SSL junction requires Certificate setup before you can create the junction. If you will be using a WebSEAL TCP junction instead of a SSL junction skip over this section and go to the "**Defining a WebSEAL TCP or SSL Junction**" section.

You must first extract the WebSphere certificate from the WebSphere server's keystore database where the ITIM Self Service Application is installed and import it into the Tivoli Access Manager WebSEAL server's keystore database.

In this example the WebSphere default **DummyServerKeyFile.jks** keystore database is being used. To verify what keystore your WebSphere Application Server is using, login to the WebSphere Administration console and then:

1. Click on the **Security** link.

2. Click on the **SSL** link.

3. Click on the ***cluster_name*/DefaultSSLSettings** link.

4. The **Key File Name** property contains the name of the keystore database file.

To extract the WebSphere certificate:

1. Start the IBM Key Management GSKit **iKeyman** utility for the WebSphere Application Server. It is normally located in the ***WAS_HOME***/java/jre/bin directory.

2. Select **Open** in the **Key Database File** menu.

3. Click on the **Browse** button and locate the WebSphere keystore file **DummyServerKeyFile.jks**. Enter the keystore password when prompted and click on the **OK** button. The password for the keystore file **DummyServerKeyFile.jks** is **WebAS**.

4. Select the WebSphere certificate and then click **Extract Certificate**.

5. On the "Extract Certificate to a File" dialog, enter the following:

   Data type

   Select Base64-encoded ASCII data.

   Certificate file name

   Enter the desired file name for the certificate.

   Location

   Enter the directory path where the certificate is to be stored.

   For this example, enter **WebSphereServerCert.arm** for the Certificate file name and store the certificate in the ***WAS_HOME*/etc** directory.

6. Click on the **OK** button.

7. Close the IBM Key Management GSKit **iKeyman** utility.

You now need to transfer the extracted certificate to the WebSEAL server and then import it into the Tivoli Access Manager WebSEAL keystore database. If you defined your own keyfiles for WebSphere and obtained a certificate from a CA, you must use the root CA's certificate which signed your WebSphere certificate in the following steps instead. This example uses the WebSEAL default keystore database **pdsrv.kdb**. Typically on Windows systems the fully qualified path is

C:\Program Files\Tivoli\PDWeb\www-default\certs\pdsrv.kdb and on UNIX/Linux systems the fully qualified path is **/var/pdweb/www-default/certs/pdsrv.kdb**.

1. On the WebSEAL server, start the IBM Key Management GSKit **iKeyman** utility.

2. Select **Open** in the **Key Database File** menu.

3. Select **CMS** for the **Key database type**.

4. Click on the **Browse** button and locate the WebSEAL keystore database file **pdsrv.kdb**. Enter the keystore password when prompted and click on the **OK** button. The password for the default WebSEAL keystore database is **pdsrv**.

5. When the database opens, select **Signer Certificates**.

6. Click on the **Add** button. The "Add CA's Certificate from a File dialog" appears.

7. Specify the following on the dialog to Add the CA's Certificate from a File:

   Data Type

   Select Base64-encoded ASCII

   Certificate file name

   Click on the **Browse** button and locate the certificate file name that you transferred from the WebSphere Server.

8. Click **OK**. A prompt appears for entry of a label name to store the certificate. Enter the desired name for the certificate (eg. WebSphere).

9. Click **OK**. The IBM Key Management panel appears with a list of Signer Certificates, including the label name that you specified.

10. Close the IBM Key Management GSKit **iKeyman** utility.

Continue to the next section: "**Defining a WebSEAL TCP or SSL Junction**".

Defining a WebSEAL TCP or SSL Junction

To simplify the examples in this section the Tivoli Access Manager **pdadmin** command utility will be used to define the Tivoli Access Manager WebSEAL junction. You could also use the Tivoli Access Manager Web Portal Manager GUI.

To create a WebSEAL junction you must know the name of your WebSEAL server. To determine the name of your WebSEAL server, issue a `server list` command from the **pdadmin>** command prompt:

```
pdadmin sec_master> server list
        amwpm-tam60-server
        ivacld-tam60-server
        default-webseald-tam60-server
pdadmin sec_master>
```

In the example above, the name of the WebSEAL server is `default-webseald-tam60-server`

Now issue the **server task create** command from the **pdadmin>** command prompt to create the junction. The command syntax is:

server task *webseal_server_name* **create** *options* ***/****junction_name*

Where:

webseal_server_name

Name of the WebSEAL server.

options

The following options are required:

-t *type*

Defines the type of junction type.
Specify **tcp** to create a TCP junction.
Specify **ssl** to create a SSL junction.

-h *hostname*

Specify the fully-qualified hostname of the Tivoli Identity Manager Server.

-p *port_number*

Specify the port number for the junction.
The default value is 80 for a TCP junction.
The default value is 9443 for an SSL junction.

-s

The junction supports stateful applications.

-j

Junction cookies are used to handle server relative URLs.

-e **utf8_uri**

utf8_uri – WebSEAL sends the headers in UTF-8 but URI also encodes them.

-c **iv_user**

iv_user – Tivoli Access Manager user account name (short form) will be provided in the **iv-user** HTTP request header

junction_name

Specify a name for the junction point. Each junction point should have a unique name.

For example, to define a TCP junction enter the following command (all on 1 line) at the **pdadmin>** command prompt:

```
server task default-webseald-tam60-server create -t tcp -s -j –e utf8_uri –c
iv_user -p 9080 -h ITIMServer.ondemandinc.com /itimserver
```

For example, to define an SSL junction:

```
server task default-webseald-tam60-server create -t ssl -s -j -e utf8_uri -c
iv_user -p 9443 -h ITIMServer.ondemandinc.com /itimserver
```

To display the WebSEAL junction issue the **show** command from the **pdadmin>** command prompt:

```
server task default-webseald-tam60-server show /itimserver
```

```
  Junction point: /itimserver
  Type: SSL
  Junction hard limit: 0 - using global value
  Junction soft limit: 0 - using global value
  Active worker threads: 0
  Basic authentication mode: filter
  Forms based SSO: disabled
  Authentication HTTP header:       insert - iv_user
  Remote Address HTTP header: do not insert
  Stateful junction: yes
  Boolean Rule Header: no
  Scripting support: yes
  Preserve cookie names: no
  Cookie names include path: no
  Transparent Path junction: no
  Delegation support: no
  Mutually authenticated: no
  Insert WebSphere LTPA cookies: no
  Insert WebSEAL session cookies: no
  Request Encoding: UTF-8, URI Encoded
  Server 1:
       ID: 57d5c862-b2ea-11db-be6a-000c29c4fcbb
       Server State: running
       Operational State: Online
       Hostname: ITIMServer.ondemandinc.com
       Port: 9443
       Virtual hostname: ITIMServer.ondemandinc.com:9443
       Server DN:
       Query_contents URL: /cgi-bin/query_contents
       Query-contents: unknown
       Case insensitive URLs: no
       Allow Windows-style URLs: yes
       Current requests : 0
       Total requests : 1
```

The Server State of the WebSEAL junction should be "**running**". If the Server State is not "**running**" then that indicates a networking type problem (eg. Invalid hostname, invalid port, WebSphere Application Server is not up and operational, network connection problem, etc.).

Defining a TAM ACL

To simplify the example in this section the Tivoli Access Manager **pdadmin** command utility will be used to define the Tivoli Access Manager ACL. You could also use the Tivoli Access Manager Web Portal Manager GUI.

Assuming you are already logged in to the **pdadmin** command utility, enter the following command (on 1 complete line) from the **pdadmin>** command prompt to create the Tivoli Access Manager ACL **ITIM-Self-Help-ACL**:

```
acl create ITIM-Self-Help-ACL
```

Grant the TAM Group access to the TAM ACL

To simplify the examples in this section the Tivoli Access Manager **pdadmin** command utility will be used to define the Tivoli Access Manager ACL. You could also use the Tivoli Access Manager Web Portal Manager GUI.

Enter the following command from the **pdadmin>** command prompt to modify the Tivoli Access Manager ACL **ITIM-Self-Help-ACL**and give the Tivoli Access Manager Group **ITIM-Self-Service-Group** the authority to **T**raverse directories, **r**ead and e**x**ecute:

```
acl modify ITIM-Self-Help-ACL set group ITIM-Self-Service-Group Trx
```

Enter the following command from the **pdadmin>** command prompt to modify the Tivoli Access Manager ACL **ITIM-Self-Help-ACL**and allow **unauthenticated users** only to **T**raverse the directory.

```
acl modify ITIM-Self-Help-ACL set any-other T
```

Enter the following command from the **pdadmin>** command prompt to modify the Tivoli Access Manager ACL **ITIM-Self-Help-ACL** and allow **users who have not been authenticated** only to **T**raverse the directory.

```
acl modify ITIM-Self-Help-ACL set unauthenticated T
```

Associate the WebSEAL Junction to the TAM ACL

To simplify the example in this section, the Tivoli Access Manager **pdadmin** command utility will be used to associate the fully qualified WebSEAL junction name which is used to access the ITIM Self Service Application to a Tivoli Access Manager ACL. You could also use the Tivoli Access Manager Web Portal Manager GUI..

The syntax of the **pdadmin** command to associate the fully qualified WebSEAL junction name of the ITIM Self Service Application to a Tivoli Access Manager ACL is:

```
acl attach prefix/webseal_junction/itim/self acl_name
```

where:

prefix is the Tivoli Access Manager Object Space ***prefix*** for your WebSEAL server. Assuming you are already logged in to the **pdadmin** command utility, enter the following command from the **pdadmin>** command prompt to display the ***prefix***:

```
object list /WebSEAL
    /WebSEAL/tam60-server-default
```

In the above example the ***prefix*** is `/WebSEAL/tam60-server-default.`

webseal_junction is the name of the WebSEAL junction you created previously with the **server task create** command. In this example, the WebSEAL junction name is **`/itimserver`.** So the fully qualified WebSEAL junction name will be: `/WebSEAL/tam60-server-default/itimserver`

acl_name is the name of the Tivoli Access Manager ACL that was created previously. In this example the name is **ITIM-Self-Help-ACL.**

Assuming you are already logged in to the **pdadmin** command utility, enter the following command (on 1 complete line) from the **pdadmin>** command prompt to associate the fully qualified WebSEAL junction name `/WebSEAL/tam60-server-default/itimserver` to the Tivoli Access Manager ACL `ITIM-Self-Help-ACL.`

```
acl attach /WebSEAL/tam60-server-default/itimserver/itim/self ITIM-Self-Help-ACL
```

Configure ITIM to use Single Sign-On

In order for Tivoli Identity Manager (and the ITIM Self Service Application) to use Single Sign-On you must make the following configuration changes to the **ui.properties** file located in the ***ITIM_HOME***/data directory:

1. Change the value of the attribute **enrole.ui.ssoEnabled** in the **ui.properties** file from **false** to **true**

   enrole.ui.ssoEnabled=**true**

2. Verify the following statement exists in the **ui.properties** file. If not add it.

   enrole.ui.ssoEncoding=**UTF-8**

3. If the **enduser.ui.ssoadapter** attribute exists in the **ui.properties** file make sure that its value is **com.ibm.itim.ui.struts.security.TAMIVHeaderSSOAdapter.** If not change the statement value, comment it out or remove it completely (as the default value for **enduser.ui.ssoadapter** is **com.ibm.itim.ui.struts.security.TAMIVHeaderSSOAdapter**).

   enduser.ui.ssoadapter=**com.ibm.itim.ui.struts.security.TAMIVHeaderSSOAdapter**

You must stop and restart the WebSphere Application Server for changes to the ***ui.properties*** file to become effective.

Accessing the ITIM Self Service Application

Once a junction has been created between the WebSEAL server and the host where the ITIM Self Service Application is running, the URL used to access the ITIM Self Service Application must include the junction name. The format of the URL is: ***protocol://host_name/junction_name*/itim/self**

protocol

The type of protocol being used. Specify either **http** or **https**.

host_name

Specify the name of the host machine where the Tivoli Access Manager WebSEAL server is installed.

junction_name

The name of the WebSEAL junction.

For example:

http://TAM60-Server/ITIMServer/itim/self

or

https://TAM60-Server/ITIMServer/itim/self

7

Problem Determination

The Self Service application has dependencies which include Tivoli Identity Manager shared libraries, compatible levels of Tivoli Identity Manager server code, and local files. Problems encountered with the ITIM Self Service application are likely due to a problem in one of these areas.

Identifying Code Level

The Self Service EAR and each JAR file contains build information in their manifest. This information will allow you to confirm the maintenance level of the code in use. To use the Tivoli Identity Manager Server and the ITIM Self Service application, the code levels must be compatible.

ManifestReader is a java application shipped with the Tivoli Identity Manager 4.6 server. It is a manifest reader program provided in the **itim_server.jar**. The ManifestReader takes file names as arguments and then displays the META-INF/MANIFEST.MF information.

To run the manifest reader utility, Java must have the **itim_server.jar** in its classpath. This is most easily accomplished by using the **-cp** option and specifying the complete path to **itim_server.jar**. The program takes file arguments for multiple files in JAR or EAR format and can be fully qualified, or specified with wildcards.

Run the manifest reader utility in the directory which you wish to examine.

ManifestReader Usage - Unix

Specifies all Self Service JAR files (ui*.jar) in the present directory:

```
java –cp /opt/IBM/itim/lib/itim_server.jar
com.ibm.itim.serviceability.ManifestReader ui*.jar
```

Note: jar files for the Self Service Application are stored in the WebSphere installedApps directory.

ManifestReader Usage - Windows

Specifies all Self Service JAR files (ui*.jar) in the present directory:

```
java -cp "c:\Program Files\IBM\itim\lib\itim_server.jar"
com.ibm.itim.serviceability.ManifestReader ui*.jar
```

Note: jar files for the Self Service Application are stored in the WebSphere installedApps directory. To examines the output of this utility for the Self Service jars, run the utility from the WebSphere installedApps directory:

```
c:\Program
Files\WebSphere\AppServer\installedApps\ITIMServer\ITIM_Self_Service.ear>
```

ManifestReader Sample Output

Following is sample output for the Self Service JAR files (ui*.jar) from the ManifestReader command.

```
File Name: ui_api.jar
Entries:   208
 IdentityManagerEndUserUIServiceability
  Build-Number=0705150831
  Build-Server=buildsvr2
  Build-User=root
  Build-Jar=ui_api.jar
  Build-Date=May 15 2007
  Build-Time=08:31 PDT

 --------------

File Name: ui_impl_enduser.jar
Entries:   856
 IdentityManagerEndUserUIServiceability
  Build-Number=0705150831
  Build-Server=buildsvr2
  Build-User=root
  Build-Jar=ui_impl_enduser.jar
  Build-Date=May 15 2007
  Build-Time=08:31 PDT

 --------------

File Name: ui_logic_enduser.jar
Entries:   321
 IdentityManagerEndUserUIServiceability
  Build-Number=0705150831
  Build-Server=buildsvr2
  Build-User=root
  Build-Jar=ui_logic_enduser.jar
  Build-Date=May 15 2007
  Build-Time=08:31 PDT

 --------------
```

Shared Library Configured

If you encounter “class not found” exceptions, the first step should include verifying your shared library configuration. The WebSphere shared library is necessary to provide the Self Service application classes which exist in the Tivoli Identity Manager server product. Refer to the installation steps for proper setup of the shared library.

ITIM Self Service Logon Page does not Load

Symptom:

If an attempt to access the ITIM Self Service user interface results in the following message being displayed in the browser window, verify the shared configuration.

> Error 503: Failed to load target servlet [action]

Action:

Ensure there are no blanks at the end of the shared library statement. Sometimes this will occur if the shared library statement was cut-and-pasted from this document.

Trace

The Tivoli Identity Manager trace facility provides methods to capture information about the Tivoli Identity Manager Server internal operations. The information that is captured within the trace log file is intended to be used by support personnel to trace a problem to its source and determine why an error occurred.

Configuration properties for the server ***trace log*** are located in the ***enRoleLogging.properties*** file. Changes are not in effect until detected by the Tivoli Identity Manager Server. The Tivoli Identity Manager Server performs periodic checks for updates based on an interval specified in the properties file.

For details of the trace facility and configuring the trace settings, refer to the *IBM Tivoli Identity Manager Server Problem Determination Guide*.

Self Service Application trace setting

For the ITIM Self Service application, new trace settings have been provided that will enable recording of trace entries specific to the Self Service Application. The entries will be recorded in the ITIM server ***trace.log*** (as configured for the server).

To enable tracing of the ITIM Self Service application, add the following entry to the ***enRoleLogging.properties*** file.

```
# Enables tracing for the ITIM Self Service application
#  The ui.struts package contains the UI logic and is the
#  preferred package to DEBUG when troubleshooting.
logger.trace.com.ibm.itim.ui.impl.level=DEBUG_MAX
logger.trace.com.ibm.itim.ui.struts.level=DEBUG_MAX
```

DEBUG_MAX is the most verbose level of logging and may have an impact on performance. This trace should only be enabled on the advice of support personnel who need the trace information to debug a problem.

Appendix A

Appendix A – Sample ACIs

ACIs for Account Operations

To use some of the Account features such as Add, Modify and Delete accounts, account ACIs need to be defined to enable these capabilities for users. When defining an account ACI, six operations can be included for the ACI definition; Search, Modify, Suspend, Add, Restore, Remove. For the Self Service Application, four of the operations are needed; Search, Modify, Add, Remove.

Self Service Feature	ACI	Operation
Request Account	Account ‘Search’ ACI	Operation = Search
	Account ‘Add’ ACI	Operation = Add
Change Account	Account ‘Search’ ACI	Operation = Search
	Account ‘Modify’ ACI	Operation = Modify
Remove Account	Account ‘Search’ ACI	Operation = Search
	Account ‘Delete’ ACI	Operation = Remove

Depending on the planned implementation, all operations can be defined on a single Account ACI or the operations can be separately defined, if needed.

When defining the Account ACI, the Class of the ACI can be set to ‘All Accounts’ or it can be set to individual account types. Using the ‘All Accounts’ class means a single ACI can be defined that applies to all accounts. While this method is simple, it does not give you read and write control over individual account attributes. To have tighter control on the attributes that are displayed and able to be modified, define Account ACIs and select individual account types for the ACI Class.

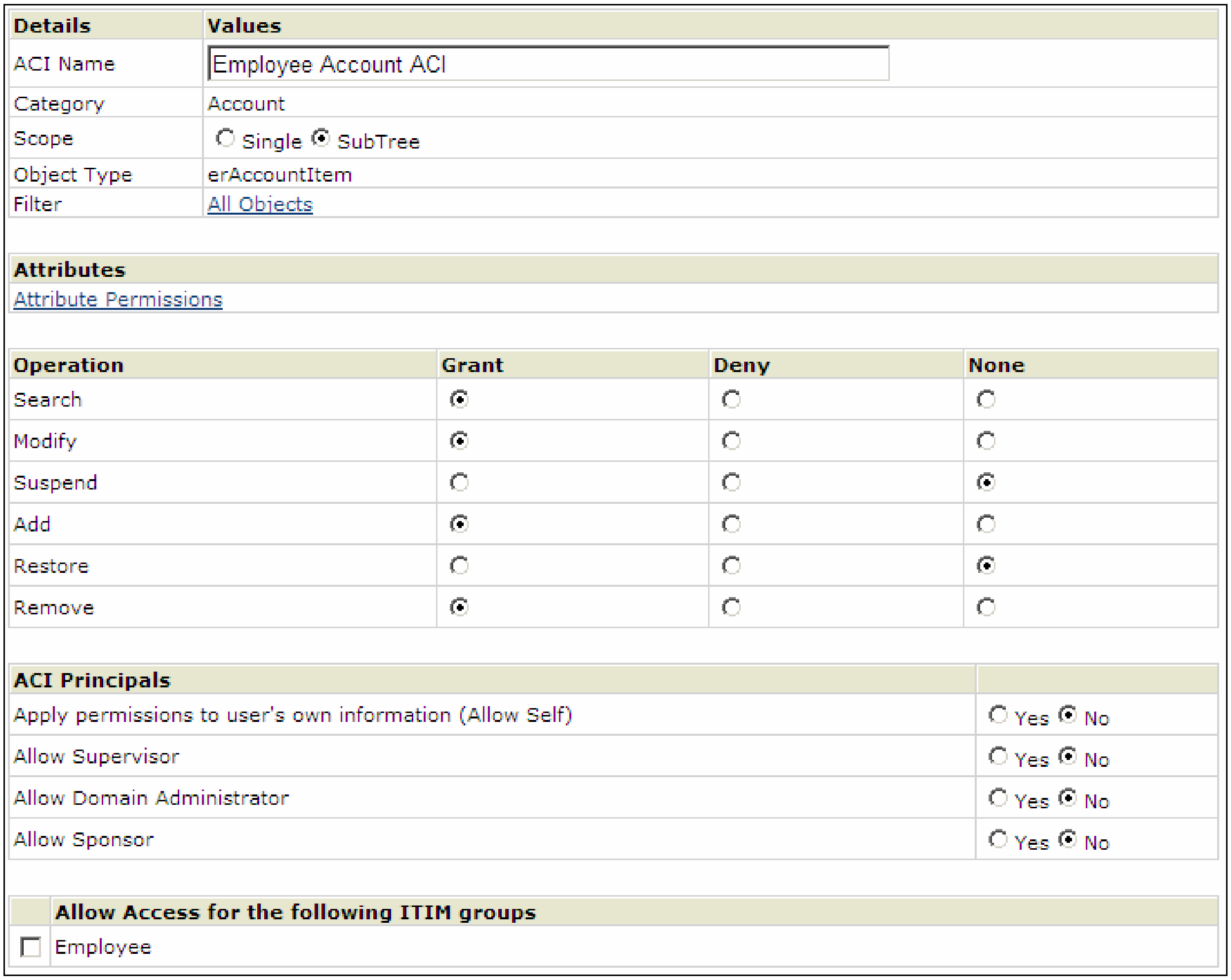
Following are a couple examples; one Account ACI with ACI Class set to ‘All Accounts’, another Account ACI with ACI Class set to WinLocalAccount.

Account ACI: Class = All Accounts

The Tivoli Identity Manager administrator defines the Account ACI by going to ‘My Organization’ and then selecting Control Access:

Select the ‘Add’ button to define a new ACI. For the category select ‘Account’; for the class of the new ACI, select ‘All Accounts’.

The following is an example of an ACI to grant Search, Modify, Add and Remove authority to users belonging to the Tivoli Identity Manager group called ‘Employee’.



Details	Values
ACI Name	Employee Account ACI
Category	Account
Scope	○ Single ● SubTree
Object Type	erAccountItem
Filter	All Objects

Attributes
Attribute Permissions

Operation	Grant	Deny	None
Search	●	○	○
Modify	●	○	○
Suspend	○	○	●
Add	●	○	○
Restore	○	○	●
Remove	●	○	○

ACI Principals	
Apply permissions to user's own information (Allow Self)	○ Yes ● No
Allow Supervisor	○ Yes ● No
Allow Domain Administrator	○ Yes ● No
Allow Sponsor	○ Yes ● No

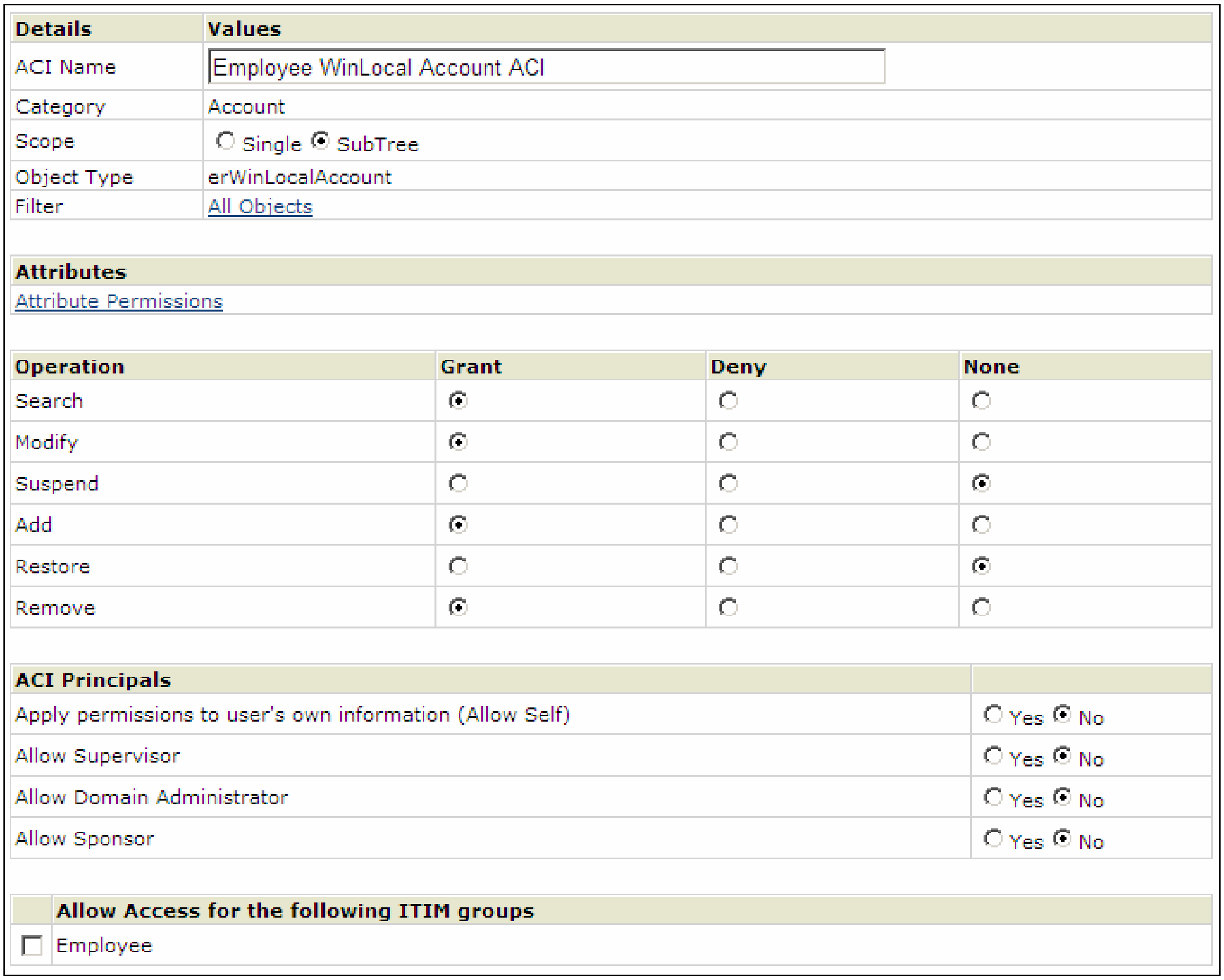
	Allow Access for the following ITIM groups
☐	Employee

On the ‘Attribute Permissions’ page, grant ‘Read’ and ‘Write’ capabilities on all the attributes that the user should have access to.

Account ACI: Class = All WinLocalAccount

If you would like to exert more control over the attributes that can be displayed and/or modified, you can create Account ACIs for specific account types.

The example below shows an ACI for the Windows Local accounts that controls the attributes that are displayed and able to be modified to users belonging to the Tivoli Identity Manager group called ‘Employee’.



Details	Values
ACI Name	Employee WinLocal Account ACI
Category	Account
Scope	○ Single ● SubTree
Object Type	erWinLocalAccount
Filter	All Objects

Attributes
Attribute Permissions

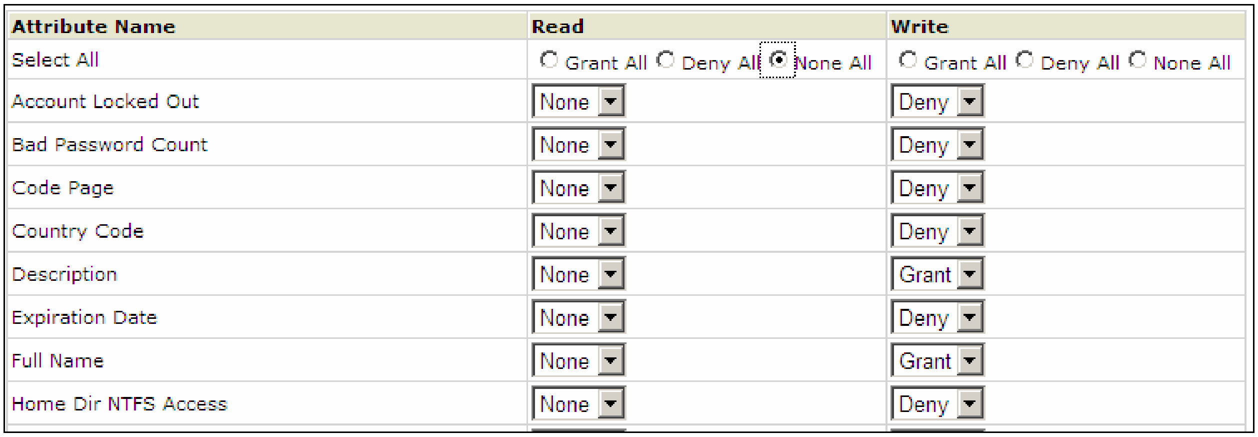
Operation	Grant	Deny	None
Search	●	○	○
Modify	●	○	○
Suspend	○	○	●
Add	●	○	○
Restore	○	○	●
Remove	●	○	○

ACI Principals	
Apply permissions to user's own information (Allow Self)	○ Yes ● No
Allow Supervisor	○ Yes ● No
Allow Domain Administrator	○ Yes ● No
Allow Sponsor	○ Yes ● No

	Allow Access for the following ITIM groups
☐	Employee

On the ‘Attribute Permissions’ page, grant ‘Read’ and ‘Write’ capabilities on all the attributes that users in the group will be allowed to view and modify.

In the example below, the ability to modify is denied for all attributes except ‘Description’ and ‘Full Name’.



Attribute Name	Read	Write
Select All	○ Grant All ○ Deny All ● None All	○ Grant All ○ Deny All ○ None All
Account Locked Out	None	Deny
Bad Password Count	None	Deny
Code Page	None	Deny
Country Code	None	Deny
Description	None	Grant
Expiration Date	None	Deny
Full Name	None	Grant
Home Dir NTFS Access	None	Deny

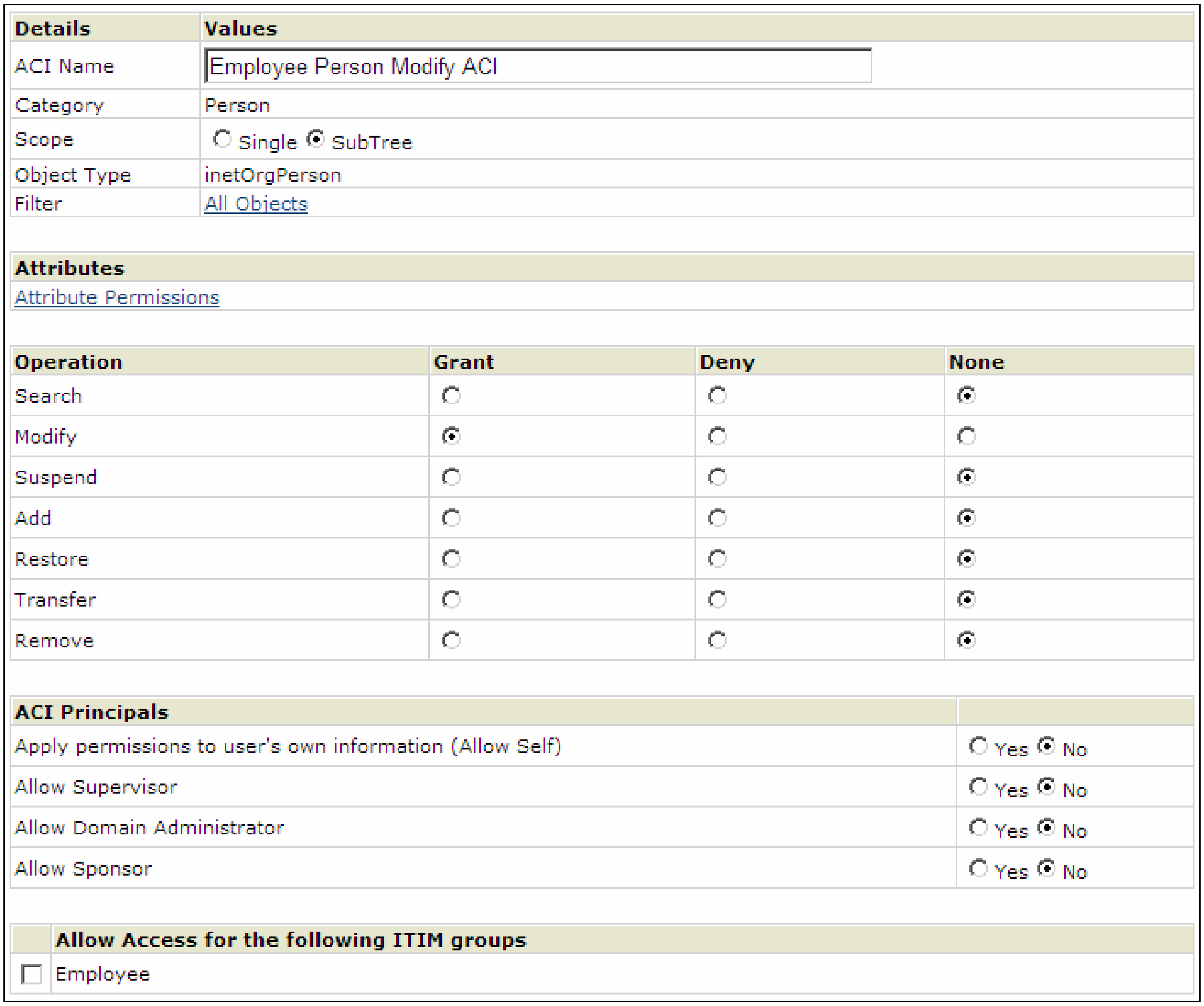
ACI for Personal Profile Updates

The default ACI “Default ACI for Person: Grant Modify and Read All Attributes to Self” provides the capability for users to view their own personal profiles.

To allow a user to change information in their personal profile, an ACI needs to be modified or a new ACI created to enable this capability.

If a new ACI is created, select ‘Person’ for the ACI category.

The following is an example of an ACI to grant Modify personal profile authority to users belonging to the Tivoli Identity Manager group called ‘Employee’.



Details	Values
ACI Name	Employee Person Modify ACI
Category	Person
Scope	○ Single ● SubTree
Object Type	inetOrgPerson
Filter	All Objects

Attributes
Attribute Permissions

Operation	Grant	Deny	None
Search	○	○	●
Modify	●	○	○
Suspend	○	○	●
Add	○	○	●
Restore	○	○	●
Transfer	○	○	●
Remove	○	○	●

ACI Principals	
Apply permissions to user's own information (Allow Self)	○ Yes ● No
Allow Supervisor	○ Yes ● No
Allow Domain Administrator	○ Yes ● No
Allow Sponsor	○ Yes ● No

	Allow Access for the following ITIM groups
☐	Employee

On the ‘Attribute Permissions’ page, grant ‘Read’ and ‘Write’ capabilities on all the attributes that users in the group will be allowed to modify.

ACIs for Delegate Operation

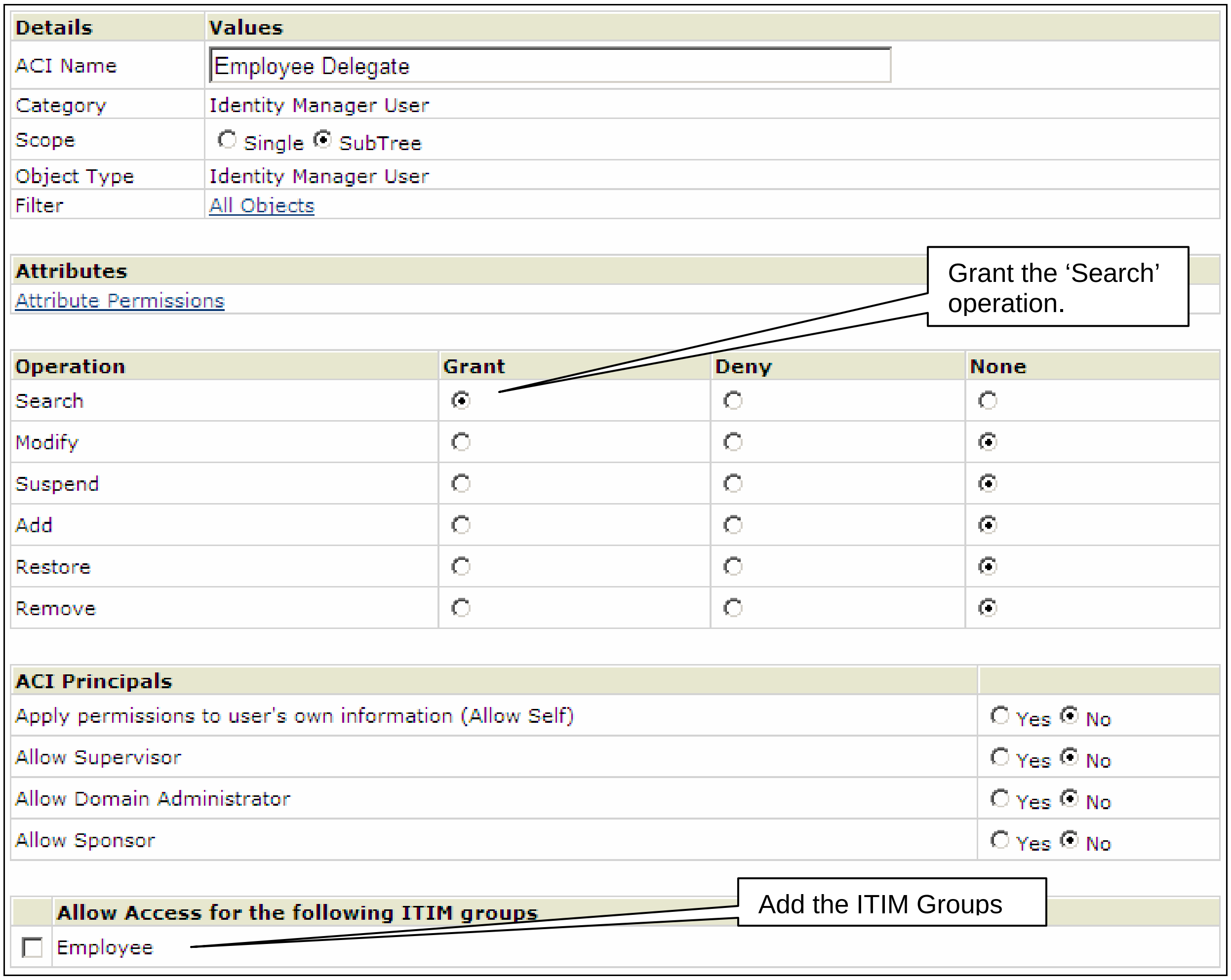
Delegate ACI

To allow a user to delegate their to-do activities, an ACI is needed to enable the delegate capability for them.

The Tivoli Identity Manager administrator defines the ACI by going to ‘My Organization’ and then selecting Control Access:

Select the ‘Add’ button to define a new ACI. Choose ‘Identity Manager User’ as the Category.

The following is an example of an ACI to grant Delegate authority to users belonging to the Tivoli Identity Manager group called ‘Employee’.



Details	**Values**
ACI Name	Employee Delegate
Category	Identity Manager User
Scope	○ Single ● SubTree
Object Type	Identity Manager User
Filter	All Objects

Attributes

Attribute Permissions

Operation	**Grant**	**Deny**	**None**
Search	●	○	○
Modify	○	○	●
Suspend	○	○	●
Add	○	○	●
Restore	○	○	●
Remove	○	○	●

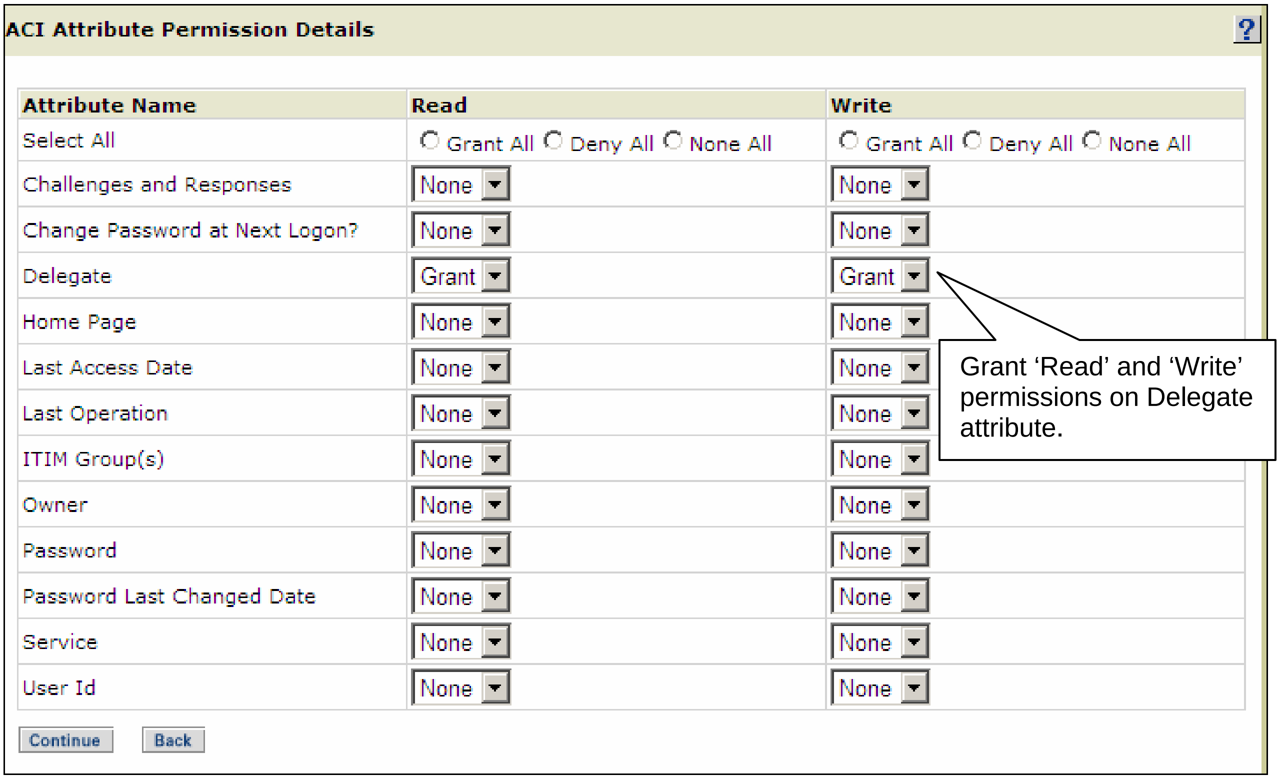
ACI Principals	
Apply permissions to user's own information (Allow Self)	○ Yes ● No
Allow Supervisor	○ Yes ● No
Allow Domain Administrator	○ Yes ● No
Allow Sponsor	○ Yes ● No

	Allow Access for the following ITIM groups
☐	Employee

Grant the ‘Search’ operation.

Add the ITIM Groups

Before saving the ACI, select the ‘Attribute Permissions’ link. Grant ‘Read’ and ‘Write’ access for the ‘Delegate’ attribute.



ACI Attribute Permission Details

Attribute Name	Read	Write
Select All	○ Grant All ○ Deny All ○ None All	○ Grant All ○ Deny All ○ None All
Challenges and Responses	None	None
Change Password at Next Logon?	None	None
Delegate	Grant	Grant
Home Page	None	None
Last Access Date	None	None
Last Operation	None	None
ITIM Group(s)	None	None
Owner	None	None
Password	None	None
Password Last Changed Date	None	None
Service	None	None
User Id	None	None

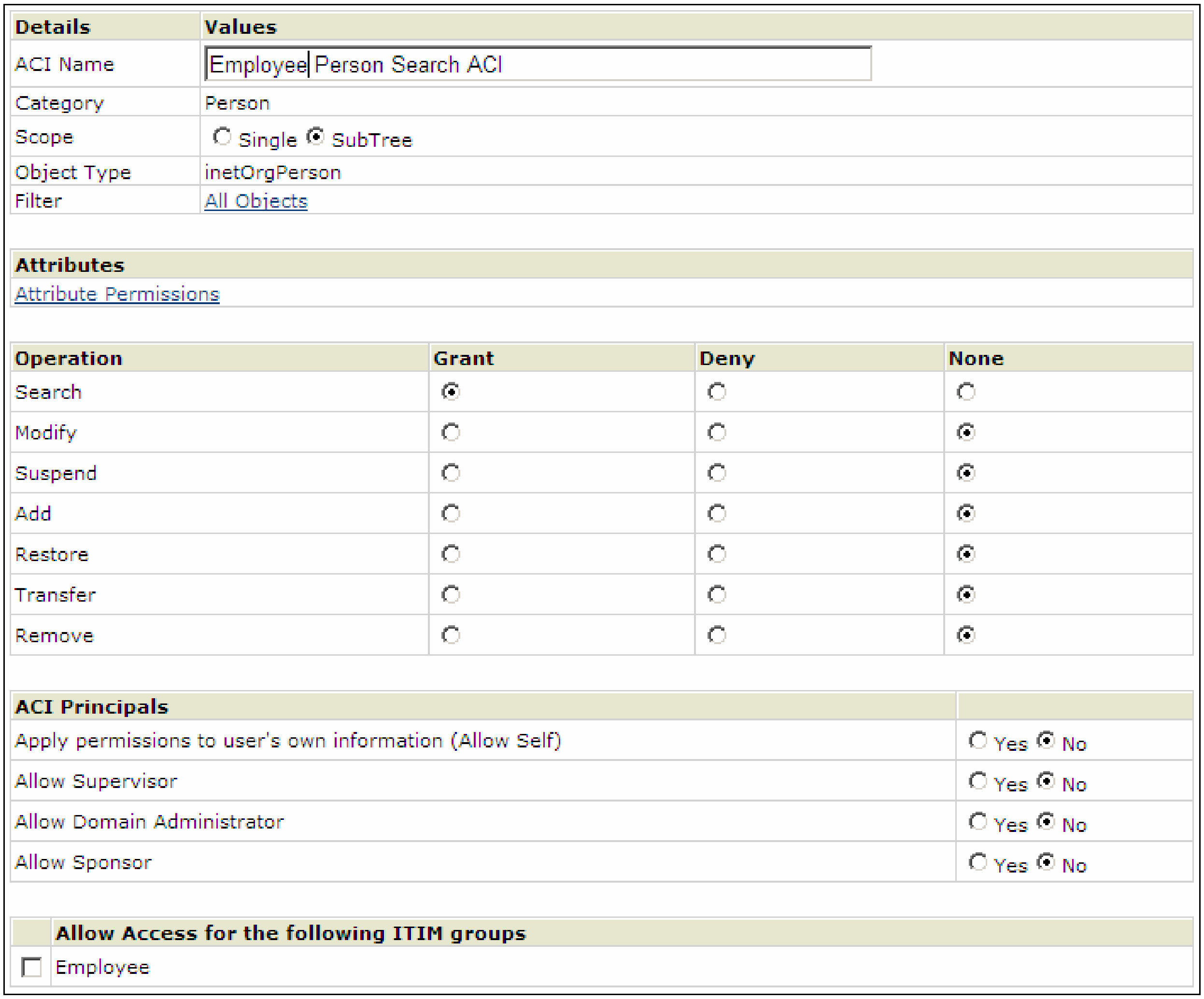
Grant ‘Read’ and ‘Write’ permissions on Delegate attribute.

Person ‘Search’ ACI

To enable users to search for people to delegate their activities to, another ACI is needed.

When creating the ACI, select ‘Person’ for the ACI category.

The following is an example of an ACI to grant Search authority to users belonging to the Tivoli Identity Manager group called ‘Employee’. This ACI is needed primarily for the Delegate capability.



Details	Values
ACI Name	Employee Person Search ACI
Category	Person
Scope	○ Single ● SubTree
Object Type	inetOrgPerson
Filter	All Objects

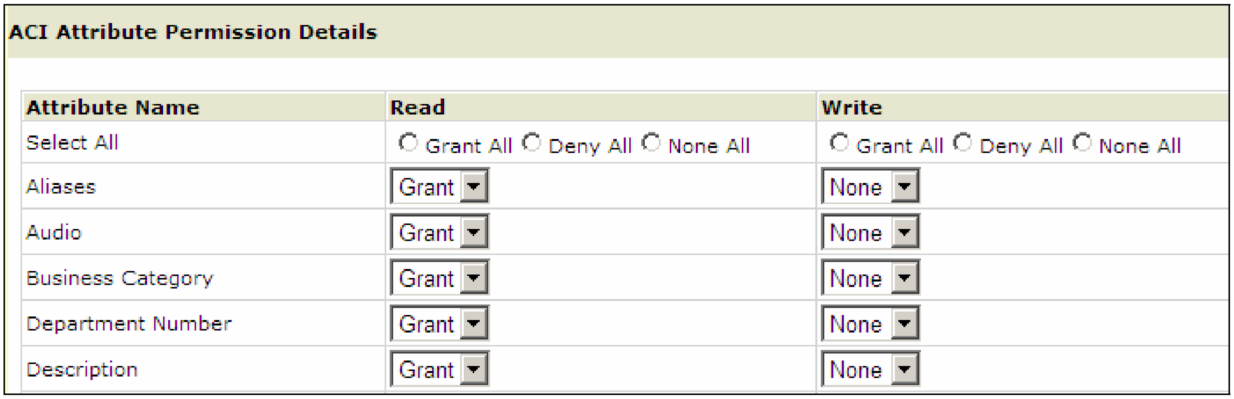
Attributes
Attribute Permissions

Operation	Grant	Deny	None
Search	●	○	○
Modify	○	○	●
Suspend	○	○	●
Add	○	○	●
Restore	○	○	●
Transfer	○	○	●
Remove	○	○	●

ACI Principals	
Apply permissions to user's own information (Allow Self)	○ Yes ● No
Allow Supervisor	○ Yes ● No
Allow Domain Administrator	○ Yes ● No
Allow Sponsor	○ Yes ● No

	Allow Access for the following ITIM groups
☐	Employee

Before saving the ACI, select the ‘Attribute Permissions’ link. Grant ‘Read’ access for all attributes.



ACI Attribute Permission Details

Attribute Name	Read	Write
Select All	○ Grant All ○ Deny All ○ None All	○ Grant All ○ Deny All ○ None All
Aliases	Grant	None
Audio	Grant	None
Business Category	Grant	None
Department Number	Grant	None
Description	Grant	None

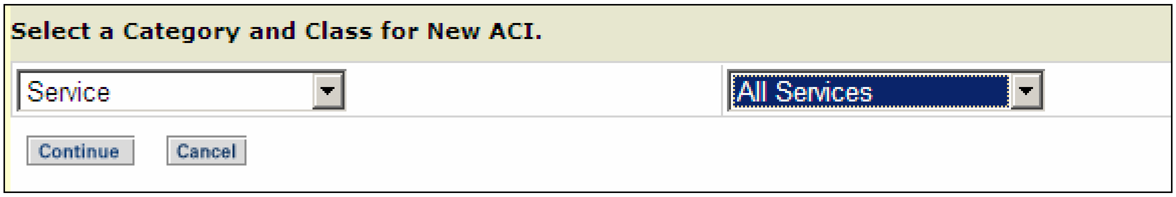
ACIs for End User Account Requests

Service ACI

To allow end users to view the service descriptions when they are requesting accounts, a service ACI needs to be defined to enable them to view the service descriptions.

This ACI is defined under ‘Provisioning’. The Tivoli Identity Manager administrator defines this ACI by going to ‘Provisioning’ and then selecting Control Access:

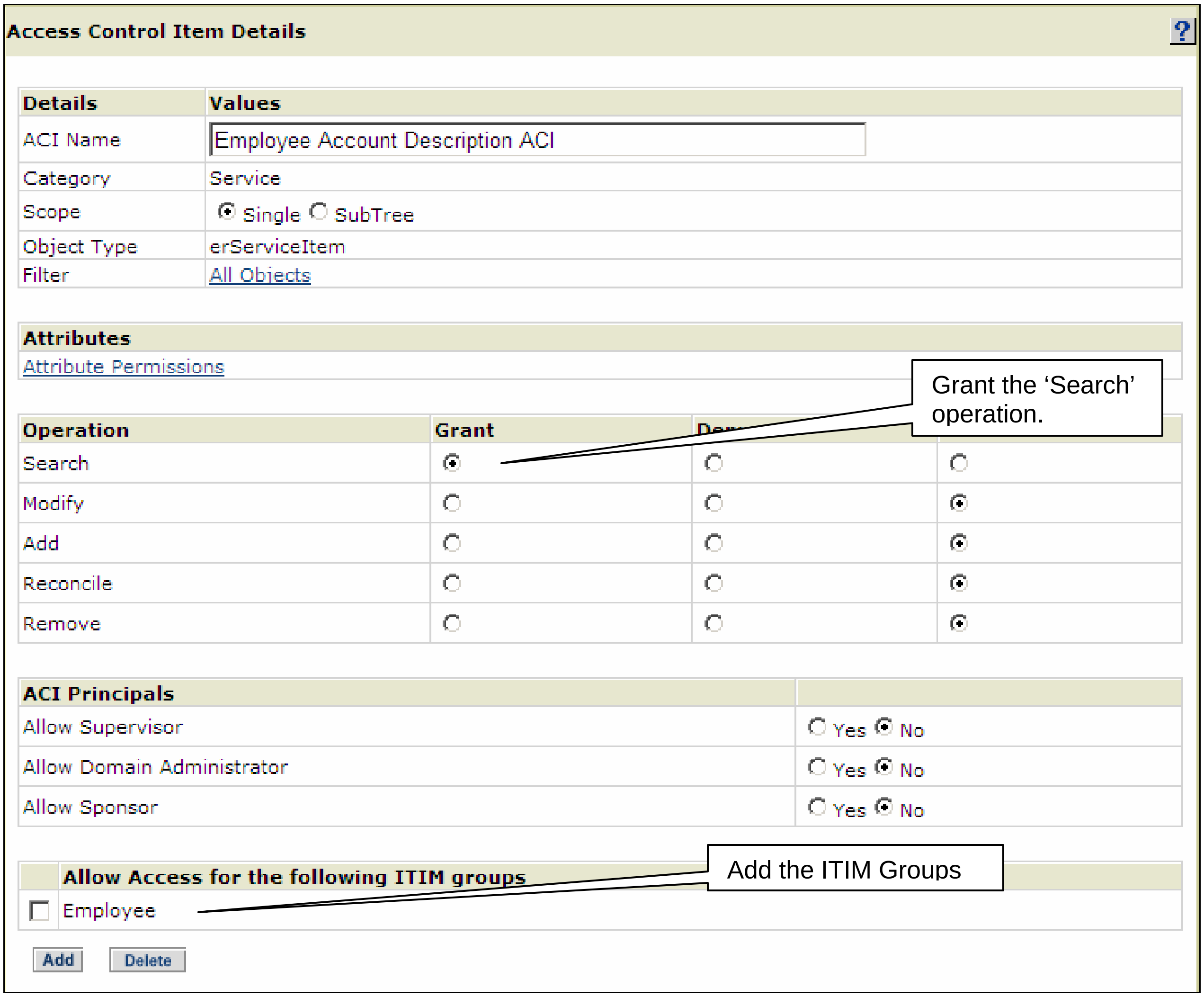
Select the ‘Add’ button to define a new ACI. Choose ‘Service’ as the Category. When prompted to ‘Select a Custom Class’, choose ‘All Services’ then select ‘Continue’.



Select a Category and Class for New ACI.

Service
All Services

The following is an example of the service ACI to grant end users the ability to view the service description when they are requesting accounts.



Access Control Item Details

Details	Values
ACI Name	Employee Account Description ACI
Category	Service
Scope	● Single ○ SubTree
Object Type	erServiceItem
Filter	All Objects

Attributes

Attribute Permissions

Grant the ‘Search’ operation.

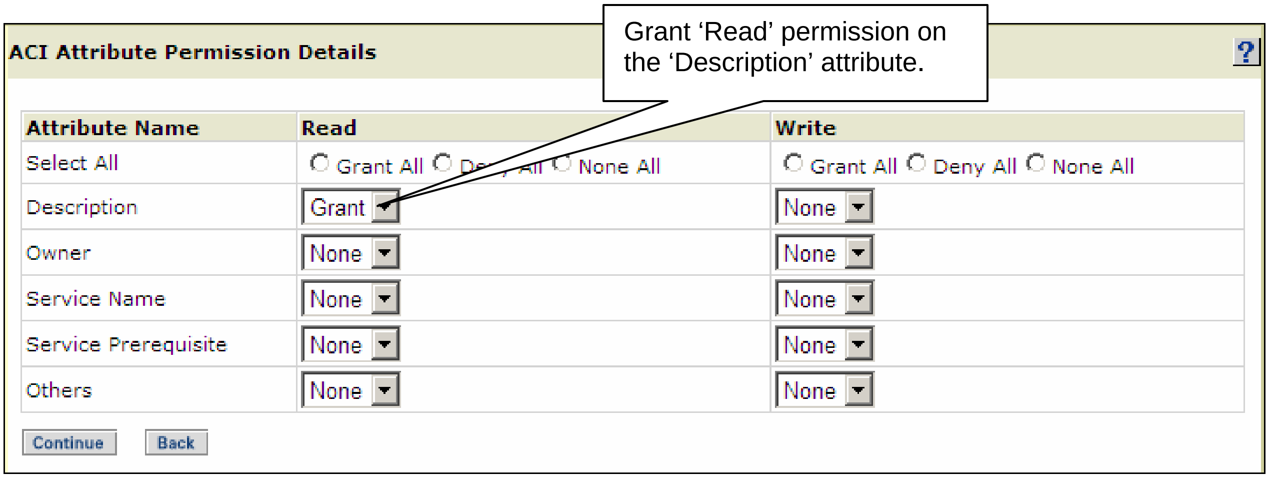
Operation	Grant	Deny	
Search	●	○	○
Modify	○	○	●
Add	○	○	●
Reconcile	○	○	●
Remove	○	○	●

ACI Principals	
Allow Supervisor	○ Yes ● No
Allow Domain Administrator	○ Yes ● No
Allow Sponsor	○ Yes ● No

Add the ITIM Groups

	Allow Access for the following ITIM groups
☐	Employee

Before saving the ACI, select the ‘Attribute Permissions’ link. Grant ‘Read’ access for the ‘Description’ attribute.



ACI Attribute Permission Details

Grant ‘Read’ permission on the ‘Description’ attribute.

Attribute Name	Read	Write
Select All	○ Grant All ○ Deny All ○ None All	○ Grant All ○ Deny All ○ None All
Description	Grant	None
Owner	None	None
Service Name	None	None
Service Prerequisite	None	None
Others	None	None

Appendix B

Appendix B - Changing Session Inactivity Timeout

A session inactivity timeout can be set for applications running on the WebSphere Application Server. If a user's session with the ITIM Self Service Application has been inactive for the specified timeout period, the session will be invalidated and the user will need to re-login the next time they interact with the application.

The default session inactivity timeout for applications is defined globally for the WebSphere Application Server and the default value is 30 minutes. When the ITIM Self Service Application is installed, it will use the timeout defined at the WebSphere Application Server level.

The session inactivity timeout for the ITIM Self Service Application can be changed using the WebSphere Administration Console. The session inactivity timeout can be changed at the **Application** level or at the **Web Modules** level (i.e. itim_self_service.war) of the application.

Once the session inactivity timeout is changed, it is necessary to restart the ITIM Self Service Application for the change to take affect. This change will need to be made each time you install/re-install the ITIM Self Service Application.

The steps below show how to change the session inactivity timeout at the Application level.

Changing Session Inactivity Timeout – WebSphere Single Server

To change the session inactivity timeout in a WebSphere Single Server Environment:

1. Login to the WebSphere Administration Console.

2. Click on the **Applications** group in the left frame, and then click on the **Enterprise Applications** link.

3. Click on the **ITIM Self Service** application link.

4. Click on the **Session Management** link.

5. Click on (check) the **Overwrite** checkbox for the **Overwrite Session Management** property.

6. Locate the **Session timeout** setting. To disable the timeout click on the "**No timeout**" radio button. To set a time interval in minutes, click on the "**Set timeout**" radio button and specify the desired time in the "**minutes**" edit box.

7. Click on the **OK** button to apply the change.

8. Click on the **Save** link and then click on the **Save** button to update the WebSphere master repository.

9. Click on the **Applications** group in the left frame, and then click on the **Enterprise Applications** link.

10. Select the checkbox next to the **ITIM Self Service** application and click on the **Stop** button.

11. Select the checkbox next to the **ITIM Self Service** application and click on the **Start** button.

Changing Session Inactivity Timeout – WebSphere Cluster

To change the session inactivity timeout in a WebSphere Cluster Environment:

1. Login to the WebSphere Administration Console.

2. Click on the **Applications** group in the left frame, and then click on the **Enterprise Applications** link.

3. Click on the **ITIM Self Service** application link.

4. Click on the **Session Management** link.

5. Click on (check) the **Overwrite** checkbox for the **Overwrite Session Management** property.

6. Locate the **Session timeout** setting. To disable the timeout click on the "**No timeout**" radio button. To set a time interval in minutes, click on the "**Set timeout**" radio button and specify the desired time in the "**minutes**" edit box.

7. Click on the **OK** button to apply the change.

8. Click on the **Save** link.

9. On the "**Save to Master Configuration**" page, ensure that the "**Synchronize changes with Nodes**" checkbox is selected and then click on the **Save** button to update the WebSphere master repository.

10. Click on the **Applications** group in the left frame, and then click on the **Enterprise Applications** link.

11. Select the checkbox next to the **ITIM Self Service** application and click on the **Stop** button.

12. Select the checkbox next to the **ITIM Self Service** application and click on the **Start** button.

Appendix C

Appendix C – Configuring Security

Administrators for the WebSphere Application Server can choose to enable Global Security and optionally, Java 2 Security. The following sections outline the steps needed to take to have the ITIM Self Service Application operate when the WebSphere Application Server has enabled Global Security and Java 2 Security.

For more information regarding configuring security for WebSphere Application Server, refer to the **WebSphere InfoCenter**:

http://publib.boulder.ibm.com/infocenter/wasinfo/v5r1//index.jsp?topic=/com.ibm.websphere.base.doc/info/welcome_base.html

Search for "**Enabling global security**".

Global Security

When the WebSphere administrator turns on Global Security, there are steps the ITIM administrator must take to enable the ITIM server to operate. The ITIM Self Service Application does not require additional configuration beyond what is done for the ITIM server. Once the steps are complete for the ITIM server, the ITIM Self Service Application should operate successfully with Global Security enabled.

Refer to the **ITIM "Server Installation and Configuration Guide for WebSphere Environments"** (SC32-1750-01) for details on how to configure the ITIM server to operate with Global Security enabled.

http://publib.boulder.ibm.com/tividd/td/ITIM/SC32-1750-01/en_US/PDF/im460_ins_ws_entprise.pdf

First, go to **Chapter 7**, "**Configuring the Tivoli Identity Manager Server**" then go to section "**Optionally configuring security after installing Tivoli Identity Manager**". Follow the steps outlined to define the 'System User' and 'EJB User'.

Next, go to **Appendix D** of the ITIM Server Installation and Configuration Guide and follow the steps outlined in the section "**Creating J2C authentication data entries**".

Java 2 Security

When Global Security is enabled for the WebSphere Application Server, Java 2 Security can optionally be enabled as well. Tivoli Identity Manager and the ITIM Self Service Application both support Java 2 Security.

It should be noted however ***that running with Java 2 Security enabled can have a significant negative performance impact on all WebSphere Applications including Identity Manager.*** Because of the performance impact, the recommendation is to run Identity Manager and the Identity Manager Self Service Application with Java 2 Security disabled on an isolated WebSphere Server. If you have a requirement to run other WebSphere Applications with Java 2 Security enabled, run them on a WebSphere Server separate from the WebSphere Server where Identity Manager is running.

If you have a requirement to run Java 2 Security for Tivoli Identity Manager and the ITIM Self Service Application, it is necessary to create a file named **library.policy** and place it in following directory:

${***WAS_HOME***}\config\cells\ ***cell_name*** \nodes\ ***node_name***

The contents of the **library.policy** file must contain these statements:

```
grant {
  permission java.security.AllPermission;
};
```

If the file is missing or missing the statement above, the ITIM Self Service Application will get Java 2 Security Exceptions when it initializes.

If you are running the IBM Tivoli Directory Server Web Administration Tool on a WepSphere Server with Java 2 Security enabled, it will be necessary to add a **permission** statement to the **was.policy** file for this application. Otherwise, it will get Java 2 Security Exceptions when it initializes. The **was.policy** file for the IBM Tivoli Directory Server Web Administration Tool is located in the following directory:

${***WAS_HOME***}\config\cells\cell_name\applications\IDSWebApp_war.ear\
deployments\IDSWebApp_war\META-INF

Add the **permission** statement below (in **bold** text) in the location indicated to the **was.policy** file

```
grant codeBase "file:${jars}" {
};

grant codeBase "file:${connectorComponent}" {
};

grant codeBase "file:${webComponent}" {
};

grant codeBase "file:${ejbComponent}" {
};

grant codeBase "file:${application}" {
  permission java.security.AllPermission;
};
```

Appendix D

Appendix D – Customization Example

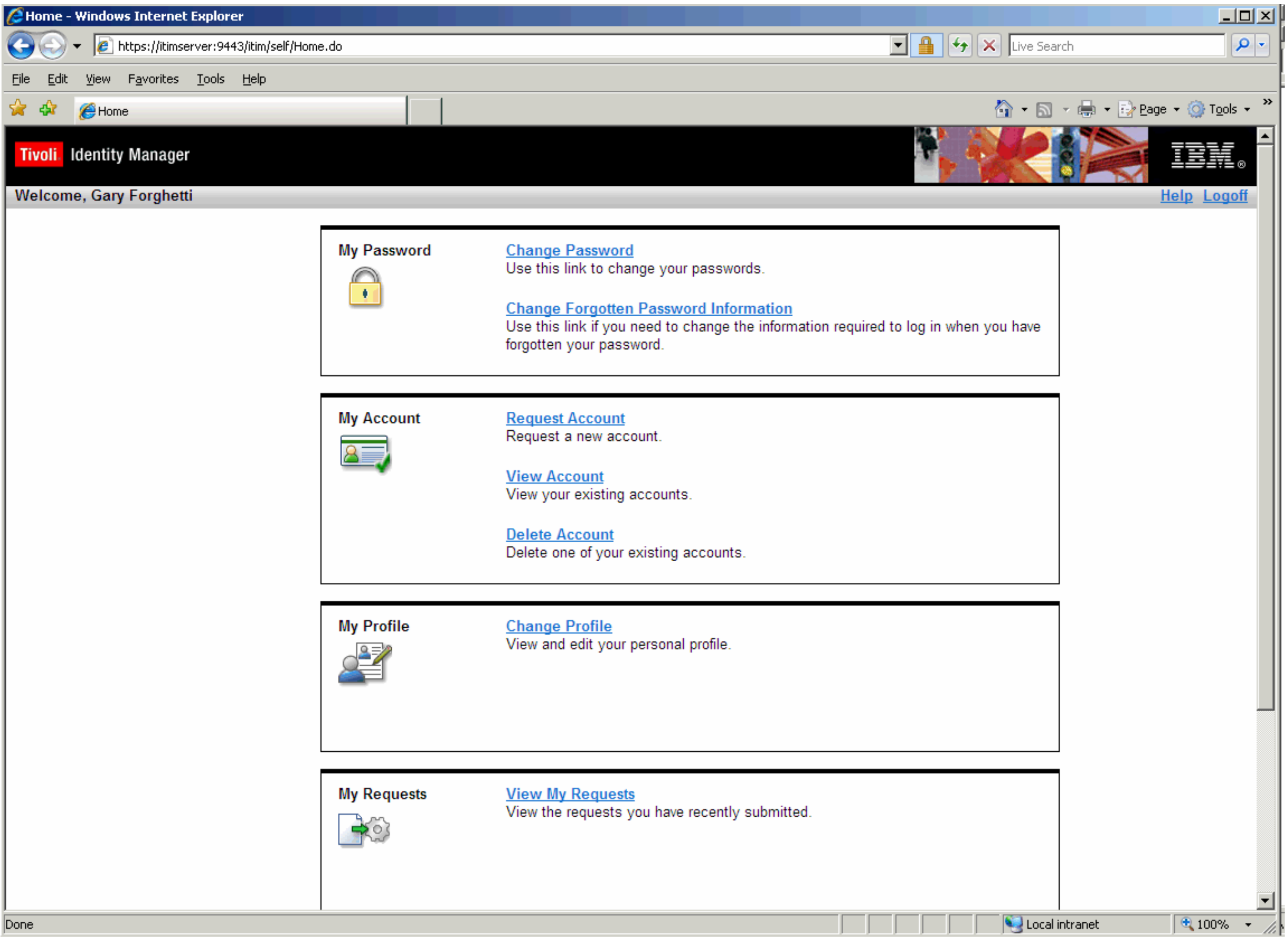
The following example will walk you through how to customize the ITIM Self Service UI Application. The following changes will be made:

1. The Background color will be changed from white to gainsboro (light gray).

2. A navigation bar will be added to the left side of every page containing simple HTML links to the tasks the user is allowed to perform.

3. The tasks will be removed from the Home page and replaced with a custom image.

Here’s is the “before” image of the ITIM Self Service Application Home page:


Home - Windows Internet Explorer
https://itimserver:9443/itim/self/Home.do
Live Search
File Edit View Favorites Tools Help
Home
Page Tools
Tivoli Identity Manager
IBM
Done
Local intranet
100%

Welcome, Gary Forghetti

Help Logoff

My Password

Change Password
Use this link to change your passwords.

Change Forgotten Password Information
Use this link if you need to change the information required to log in when you have forgotten your password.

My Account

Request Account
Request a new account.

View Account
View your existing accounts.

Delete Account
Delete one of your existing accounts.

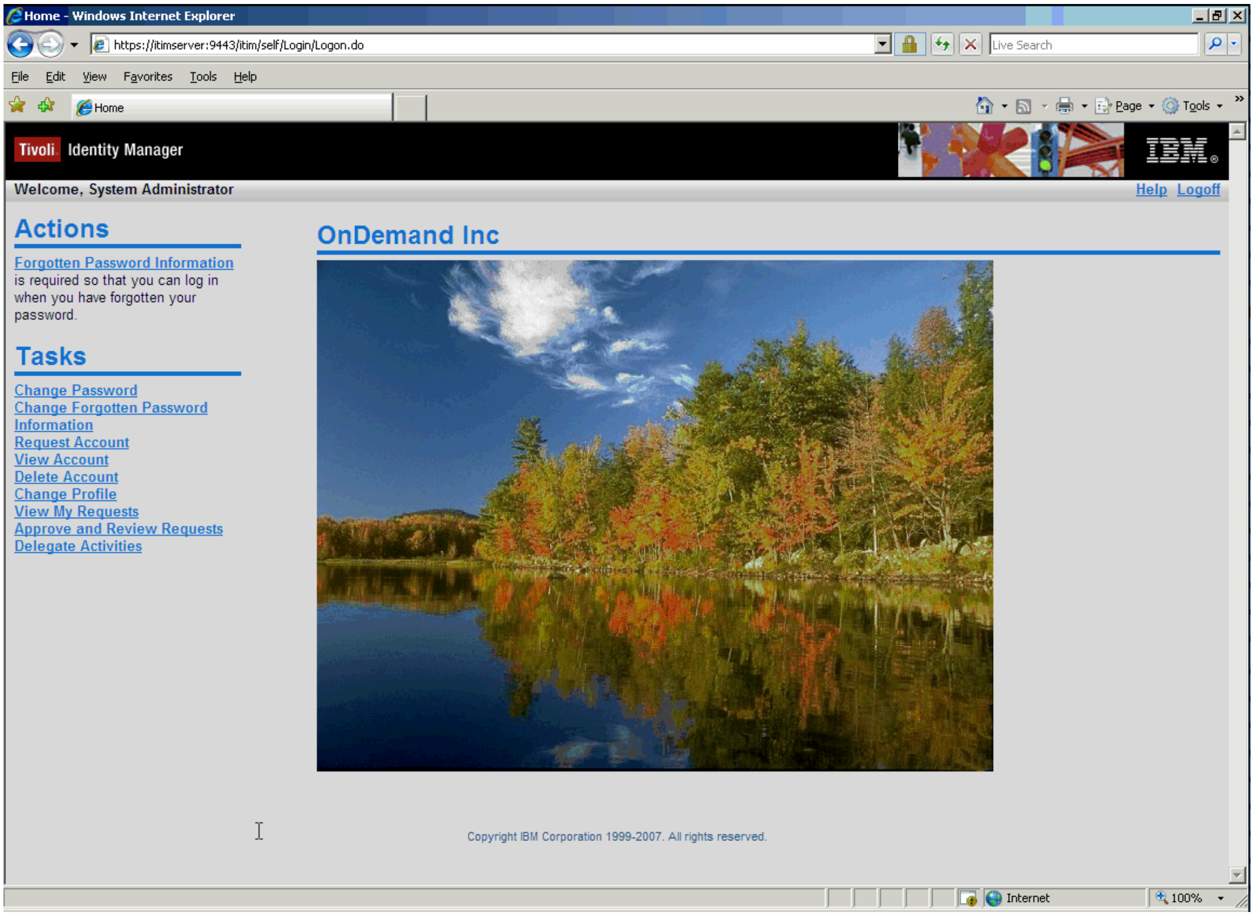
My Profile

Change Profile
View and edit your personal profile.

My Requests

View My Requests
View the requests you have recently submitted.

Here is the “after” image of the ITIM Self Service Application Home page:


Home - Windows Internet Explorer
https://itimserver:9443/itim/self/Login/Logon.do
Live Search
File Edit View Favorites Tools Help
Home
Page Tools
Tivoli Identity Manager
IBM
Welcome, System Administrator
Help Logoff
Actions
Tasks
Change Password
Change Forgotten Password Information
Request Account
View Account
Delete Account
Change Profile
View My Requests
Approve and Review Requests
Delegate Activities
OnDemand Inc
Internet
100%

Forgotten Password Information is required so that you can log in when you have forgotten your password.

Copyright IBM Corporation 1999-2007. All rights reserved.

To perform the customization the following files will need to be edited with a text editor:

- enduser.css
- nav.jsp
- SelfServiceUI.properties
- Home.jsp

If you make any mistakes, there are original copies of the above files in the directory, **<ITIM_HOME>/defaults**.

For more details regarding customization, refer to Chapter 5, Customization.

How to change the background color

To change the background color of all the ITIM Self Service Application pages, you need to edit the file **enduser.css** which resides in the following directory.

1. Edit the style sheet file, **enduser.css**

The **enduser.css** file is located in the directory

```
<WAS_HOME>\installedApps\<WAS_NODE>\
   ITIM_Self_Service.ear\itim_self_service.war\custom
```

2. Locate the following statement:

   ```
   body {
         margin: 0px 0px 0px 0px;
   }
   ```

3. Add the **background-color** attribute to the body. The new statement should look like this:

   ```
   body {
         margin: 0px 0px 0px 0px;
         background-color: gainsboro;
   }
   ```

4. Locate the following statement:

   ```
   .leftNav #nav {
         width: 100px;
         float: left;
   }
   ```

5. Add the **padding-left** attribute to the body with a padding value of 8 pixels. This will cause the Navigation Bar to be placed 8 pixels from the left side of the page. The new statement should look like this:

   ```
   .leftNav #nav {
         width: 100px;
         float: left;
         padding-left: 8px;
   }
   ```

6. Locate the following statement:

   ```
   .leftNav #content {
              margin-left: 105px;
   }
   ```

7. Change the number of pixels for the margin-left attribute from **105** to **280** which will push the content of the pages an additional 175 pixels to the right making room for the Navigation Bar. The new statement should look like this:

   ```
   .leftNav #content {
              margin-left: 280px;
   }
   ```

8. Save the changes to the file.

How to add the Navigation Bar

To add the Navigation Bar to all of the ITIM Self Service Application pages requires you to do the following:

1. Edit the file **SelfServicesUI.properties**

   The **SelfServicesUI.properties** file is located in the directory the **<ITIM_HOME>/data**

2. Locate the following statement:

   ```
   ui.layout.showNav=false
   ```

3. Change the value from **false** to **true**. The new statement should look like this:

   ```
   ui.layout.showNav=true
   ```

4. Save the changes to the file.

5. Edit the file **nav.jsp** and remove all of the existing statements in the file. The **nav.jsp** file is located in the directory

```
<WAS_HOME>\installedApps\<WAS_NODE>\
        ITIM_Self_Service.ear\itim_self_service.war\custom
```

   Remove all of the existing statements in the file.

6. Add the following statements:

```
<%@ taglib uri="http://java.sun.com/jstl/core" prefix="c"%>
<%@ taglib uri="http://java.sun.com/jstl/fmt" prefix="fmt"%>
<%@ taglib uri="http://struts.apache.org/tags-tiles-el" prefix="tiles"%>
<%@ taglib uri="http://struts.apache.org/tags-logic-el" prefix="logic"%>
<%@ taglib uri="http://struts.apache.org/tags-html-el" prefix="html"%>
<%@ taglib uri="http://struts.apache.org/tags-bean-el" prefix="bean"%>

<c:set var="pageConfig" value="${HomePageForm}" scope="page" />

<div class="MyActionSectionLinks" style="width: 210px;">
<%
    int activities = 0;
    int tasks = 0;
%>
<c:forEach items="${pageConfig.sections}" var="section">
<%--if the section has at least 1 viewable task then render the section --%>
    <c:if test="${!empty pageConfig.sectionToTaskMap[section]}">
      <c:forEach items="${pageConfig.sectionToTaskMap[section]}" var="task">
            <c:choose>
                <c:when test="${section == pageConfig.actionNeededSection}">
                <%
                    activities = activities + 1;
                    if (activities == 1)
                    {
                        out.println("<h1>Actions</h1>");
                    }
                %>
                      <c:out value="${task}" escapeXml="false" /><br><br>
                </c:when>
                <c:otherwise>
                <%
                    tasks= tasks + 1;
                    if (tasks == 1)
                    {
                        out.println("<h1>Tasks</h1>");
                    }
                %>
```

```
                    <a href="/itim/self/<c:out value="${task.urlPath}"/>">
                              <fmt:message key="${task.urlKey}" /></a><br>
                </c:otherwise>
            </c:choose>
        </c:forEach>
      </c:if>
</c:forEach>
</div>
```

7. Save the changes to the file.

How to change the Home Page

To remove the tasks from the Home Page and replace them with an image, you must do the following:

1. Put your desired image in the images directory. The images directory is

   <WAS_HOME>`\installedApps\`***<WAS_NODE>***`\`
   `ITIM_Self_Service.ear\itim_self_service.war\images`

   The file name of the image in this exercise is **mh.jpg**.

2. Edit the file **Home.jsp** and remove all of the existing statements in the file.

   The file **Home.jsp** is located in the directory

   <WAS_HOME>`\installedApps\`***<WAS_NODE>***`\`
   `ITIM_Self_Service.ear\itim_self_service.war\custom`

3. Add the following statements below. The **<img>** statement below specifies the image.

   ```
   <%@ taglib uri="http://java.sun.com/jstl/core" prefix="c"%>
   <%@ taglib uri="http://java.sun.com/jstl/fmt" prefix="fmt"%>
   <%@ taglib uri="http://struts.apache.org/tags-tiles-el" prefix="tiles"%>
   <%@ taglib uri="http://struts.apache.org/tags-logic-el" prefix="logic"%>
   <%@ taglib uri="http://struts.apache.org/tags-html-el" prefix="html"%>
   <%@ taglib uri="http://struts.apache.org/tags-bean-el" prefix="bean"%>
   <%@ include file="/jsp/common/MessageBox.jsp" %>

   <c:set var="pageConfig" value="${HomePageForm}" scope="page" />
   <br>
   <h1>OnDemand Inc</h1>
   <img style="height: 80%; auto: 80%" src="/itim/self/images/mh.jpg">
   ```

4. Save the changes to the file.

Login to the ITIM Self Service Application and you should see the new customized look. You may need to clear the cache in your Web Browser.

Notices

Notices for Tivoli Identity Self Service Application

This information was developed for products and services offered in the U.S.A. IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to: IBM Director of Licensing IBM Corporation North Castle Drive Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:IBM World Trade Asia Corporation Licensing 2-31 Roppongi 3-chome, Minato-ku Tokyo 106-0032, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged should contact:

IBM Corporation 2ZA4/101 11400 Burnet Road Austin, TX 78758 U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this information and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and

Trademarks