

IBM Security Access Manager

Versions 6.1.1, 7.0 and 8.0

Oracle PeopleSoft PeopleTools Integration Guide



Note:

Before using this information and the product it supports, read the information in [Notices](#).

This edition applies to Version 6.1 release i of the IBM Security Access Manager Integration with Oracle PeopleSoft PeopleTools and to all subsequent releases and modifications until otherwise indicated in new editions.

Copyright International Business Machines Corporation 2012, 2014.

US Government Users Restricted Rights -- Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Preface.....	5
Access to publications and terminology.....	5
Publication Library.....	5
IBM Terminology website.....	6
Accessibility.....	6
Technical training.....	7
Support information.....	7
Statement of Good Security Practices.....	7
Product name updates.....	7
Chapter 1: Introducing the Integration.....	8
Introduction.....	8
Integration product version information.....	9
Integration product contents.....	9
Before you start.....	9
Chapter 2: IBM Security Access Manager Configuration.....	10
Web Gateway Appliance Configuration.....	10
Junction Management.....	10
Web Reverse Proxy Configuration Options.....	11
Configuring the IBM Security Access Manager Logout Page.....	12
WebSEAL Configuration.....	14
Junction Creation.....	14
WebSEAL Configuration Options.....	15
Configuring the WebSEAL Logout Page.....	16
Chapter 3: Oracle PeopleSoft PeopleTools Configuration.....	18
Creating a New User Profile.....	18
Update the PeopleTools Configuration.....	18
Create the SignOn PeopleCode.....	20
Enable the SignOn PeopleCode.....	21
Modify PeopleTools Session Expiration (Standard and Transparent Path WebSEAL Junctions).....	21
Restart Application Servers.....	23
Updating PeopleSoft PeopleTools Launch URLs.....	24
Validating the Integration.....	24
Removing the Integration.....	24
Chapter 4: Troubleshooting.....	26
Collecting Support Data.....	26
Configuring PeopleCode trace.....	26
TivoliSSO PeopleCode trace overview.....	26
Disabling TivoliSSO PeopleCode trace.....	27
Minimal or incomplete user options.....	28
Logged warnings.....	28
Problems creating user profile.....	29
Problems related to the log in or log off process.....	29

PeopleTools inactivity warning.....	30
Filtering the ‘text/plain’ HTTP Content-Type.....	30
HttpOnly Cookies.....	31
Notices.....	33
Trademarks.....	36

Preface

Access to publications and terminology

The following publications complement the information contained in this document:

Publication Library

These publications complement the information that is contained in this publication:

Base Information

- *IBM® Tivoli® Access Manager Base Installation Guide*

Explains how to install, configure, and upgrade Access Manager software, including the Web portal manager interface.

- *IBM Security Access Manager Base Administrator's Guide*

Describes the concepts and procedures for using Access Manager services. Provides instructions for managing tasks from the Web portal manager interface and by using the **pdadmin** command.

WebSEAL Information

- *IBM Security Access Manager WebSEAL Installation Guide*

Provides installation, configuration, and removal instructions for the WebSEAL server and the WebSEAL application development kit.

- *IBM Security Access Manager WebSEAL Administrator's Guide*

Provides background material, administrative procedures, and technical reference information for using WebSEAL to manage the resources of your secure Web domain.

- *IBM Security Access Manager WebSEAL Developer's Reference*

Provides administration and programming information for the Cross-domain Authentication Service (CDAS), the Cross-domain Mapping Framework (CDMF), and the Password Strength Module.

Web Gateway Appliance Information

- *IBM Security Access Manager Web Gateway Appliance Administration Guide*

Provides information about configuring and maintaining a Security Access Manager environment.

- *IBM Security Web Gateway Appliance Configuration Guide for Web Reverse Proxy*

Provides configuration procedures and technical reference information for the Web Gateway Appliance.

- *IBM Security Web Gateway Appliance Web Reverse Proxy Stanza Reference*

Provides a complete stanza reference for the Web Gateway Appliance Web Reverse Proxy.

Mobile Information

- *IBM Security Access Manager for Mobile Administration Guide*

Describes how to manage, configure, and deploy an existing IBM Security Access Manager environment.

- *IBM Security Access Manager for Mobile Configuration Guide*

Explains how to complete the initial configuration of IBM Security Access Manager for Mobile.

IBM Terminology website

The IBM Terminology website consolidates terminology for product libraries in one location. You can access the Terminology website at <http://www.ibm.com/software/globalization/terminology>.

Accessibility

Accessibility features help users with a physical disability, such as restricted mobility or limited vision, to use software products successfully. With this product, you can use assistive technologies to hear and navigate the interface. You can also use the keyboard instead of the mouse to operate all features of the graphical user interface.

Technical training

For technical training information, see the following IBM Education website at <http://www.ibm.com/software/tivoli/education>.

Support information

IBM Support provides assistance with code-related problems and routine, short duration installation or usage questions. You can directly access the IBM Software Support site at <http://www.ibm.com/software/support/probsub.html>.

Statement of Good Security Practices

IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Product name updates

This publication was first established for IBM Tivoli Access Manager. IBM Tivoli Access Manager has since been superseded by IBM Security Access Manager.

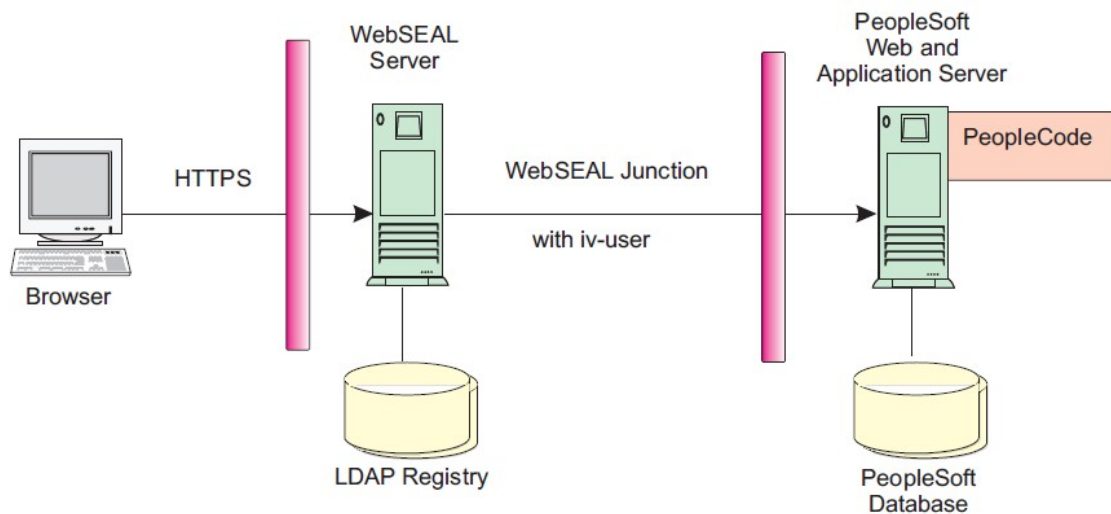
Wherever in this guide, any figures and graphics that contain or refer to IBM Tivoli Access Manager, the use of IBM Security Access Manager is implied. There are no functionality discrepancies between IBM Tivoli Access Manager and IBM Security Access Manager.

Chapter 1: Introducing the Integration

Introduction

This guide describes the integration steps that are required to achieve Single Sign-On (SSO) between IBM Security Access Manager and Oracle PeopleSoft PeopleTools.

This integration provides SSO by deploying IBM Security Access Manager as a reverse-proxy server in front of the PeopleSoft Web Application Server. IBM Security Access Manager acts as a security gateway between the client browser and the PeopleSoft Web Application Server, where it authenticates and authorizes users attempting to access PeopleTools applications. PeopleTools must be configured for delegated authentication performed by IBM Security Access Manager using custom PeopleCode.



The diagram above shows the integration architecture, which supports the following processes:

1. A client accesses PeopleTools applications through IBM Security Access Manager.
2. IBM Security Access Manager intercepts the request, authenticates and authorizes the user.
3. On successful authentication, IBM Security Access Manager passes the request to the PeopleTools application, together with the authenticated user ID in a HTTP Request header.
4. PeopleTools is configured to accept and trust the user ID from IBM Security Access Manager using custom PeopleCode.
5. The PeopleTools Application Server logs in the user and grants access.

Integration product version information

For information about the supported product versions, see the Release Notes.

Integration product contents

The integration solution is packaged as a compressed file. The package contains the following files:

Table 1. Integration product contents

File name	Description
6.1-PSPT.README	README file.
am_peopletools_int_guide.pdf	This document.
isViaWebSEAL.javascript	Sample code provided to update the PT_SAVEWARNINGSCRIPT definition.
logout.html	Updated logout page to replace in WebSEAL to invalidate cookies within the user browser.
logout_redirect.html	Sample logout redirection page used by PeopleTools to provide automated redirection to the WebSEAL logout page.
tivoliSSO.peoplecode	Sample code provided for the <i>tivoliSSO()</i> function.

Before you start

This guide does not cover the configuration of the entire environment. In particular, the following product installations and configurations must already be complete:

IBM Security Access Manager

IBM Security Access Manager Web Gateway Appliance or WebSEAL is installed and configured.

PeopleSoft PeopleTools

PeopleSoft PeopleTools should be installed and configured, including all of its dependencies.

Chapter 2: IBM Security Access Manager Configuration

Complete the following configuration steps on [Web Gateway Appliance Configuration](#) or [WebSEAL Configuration](#) for integration with **PeopleSoft PeopleTools**.

Web Gateway Appliance Configuration

It is recommended that Forms authentication is used so that single sign-out can be achieved with **PeopleSoft PeopleTools**. To disable Basic Authentication and enable Forms Authentication:

1. Open the Web Gateway Appliance Web console.
2. Select **Secure Web Settings** → **Reverse Proxy**.
3. Select the preferred instance.
4. Select **Edit**.
5. Select the **Authentication** tab.
6. Under **Basic Authentication** → **Transport**, select **None**.
7. Under **Forms** → **Forms Authentication**, select **Both**.
8. Click **Save**.
9. Deploy the pending changes.
10. Restart the reverse proxy instance.

If Forms Authentication is not used the browser window must be closed to terminate the IBM Security Access Manager session.

Junction Management

The selection of the most appropriate junctions for each environment is outside the scope of this integration. See the [IBM Security Access Manager Knowledge Center Junctions](#) page for details of each junction type.

The following example uses Transparent Path junctions to eliminate the requirement of path filtering. The Transparent Path junction name must exactly match the Context Root for PeopleSoft PeopleTools. For example, /psp.

For PeopleSoft, there are a number of root directories that will need to be accessed. These may differ depending on your PeopleSoft environment but at a minimum create transparent junctions for:

/psp
/cs

/ps
/psc

Create a transparent path junction to the PeopleSoft PeopleTools Gateway URL.

1. Open the Web Gateway Appliance Web console.
2. Select **Secure Web Settings** → **Reverse Proxy**.
3. Select the preferred instance.
4. Select **Manage** → **Junction Management**.
5. Select **New** → **Standard Junction**.
6. On the Junction tab
 - a) Add the junction name /psp
 - b) Click **Create Transparent Path Junction**.
 - c) For Junction Type, select **TCP**.
7. On the Servers tab
 - a) Click **New** to add a target backend server.
 - b) Specify the connection details of the **PeopleSoft PeopleTools** URL:
 - ◆ Hostname: pt.ibm.com
 - ◆ TCP or SSL Port: 443
 - ◆ Virtual Host: webseal.ibm.com
 - c) Click **Save**.
8. On the Identity tab
 - a) Select **HTTP Header Identity Information: IV-USER**
9. Click **Save**.
10. Create a transparent path junction for each of the PeopleTools application paths.

After creating the junctions, proceed to [Web Reverse Proxy Configuration Options](#).

Web Reverse Proxy Configuration Options

Edit the Web Reverse Proxy configuration file, modifying the following entries:

1. Open the Web Gateway Appliance Web console.
2. Select **Secure Web Settings** → **Reverse Proxy**.
3. Select the preferred instance.
4. Select **Manage** → **Configuration** → **Edit Configuration File**.

Within the **[script-filtering]** stanza, enable the `script-filter` and `rewrite-absolute-with-absolute` parameters. For example:

```
[script-filtering]
script-filter=yes
...
rewrite-absolute-with-absolute=yes
```

If the PeopleSoft application server hosts the PeopleSoft portal server, ensure that the WebSEAL authentication method and corresponding configuration will use HTTP cookies for session management. If WebSEAL is configured to use SSL, ensure that the `ssl-id-sessions` parameter is set to `no`:

```
[session]
ssl-id-sessions = no
```

5. Deploy the pending changes.
6. Restart the reverse proxy instance.

After modifying the Web Reverse Proxy Configuration Options, proceed to [Configuring the IBM Security Access Manager Logout Page](#).

Configuring the IBM Security Access Manager Logout Page

When a user successfully logs on to IBM Security Access Manager, and in turn through Single Sign-On (SSO) to PeopleTools, a session cookie from PeopleTools is stored in the browser's memory. Unless the user physically closes the browser, the session between the browser and PeopleTools remains open, even if the user has logged out of IBM Security Access Manager.

If another user were to re-use the same browser instance to log on to IBM Security Access Manager and access PeopleTools, PeopleTools may incorrectly identify the new user as the previous user due to the valid PeopleTools cookie.

To resolve this issue, the integration package includes a `logout.html` file, based on the default IBM Security Access Manager logout page. The supplied `logout.html` page includes JavaScript that invalidates session cookies from the browser upon logout from IBM Security Access Manager.

Note: IBM Security Access Manager returns the `logout.html` page when a user logs out using the `pkmslogout` function. This function is not available when IBM Security Access Manager has been configured to use the Basic Authentication (BA) authentication method. Hence this section is not relevant if IBM Security Access Manager is set to this mode.

To configure the IBM Security Access Manager logout page with the required JavaScript:

1. Make a backup copy of your existing logout page:
 - a) Open the Web Gateway Appliance Web console.
 - b) Select **Secure Web Settings** → **Reverse Proxy**.
 - c) Select the preferred instance.

- d) Select **Manage** → **Management Root**.
 - e) Select **Management** → **C** → **logout.html**
 - f) With the **logout.html** file highlighted, select **Manage** → **Export** to save the file.
2. Locate the logout.html file in the integration package.
 3. Modify the logout.html file, updating the exception_list variable to include the list of cookies that you do not want destroyed:

```
// IBM Security Access Manager Integration
// for PeopleSoft
//
// Set this variable to a semi-colon list of the names of
// cookies you do not want to delete.
var exception_list = "";
```

4. Use this logout.html file to overwrite the existing logout.html file.
5. Save the modified logout.html.
6. Deploy the pending changes.
7. Restart the reverse proxy instance.

If you have previously modified the default logout.html file, you can still add the required JavaScript functionality without abandoning your modifications. To do this:

1. Make a backup copy of your existing logout page:
 - a) Open the Web Gateway Appliance Web console.
 - b) Select **Secure Web Settings** → **Reverse Proxy**.
 - c) Select the preferred instance.
 - d) Select **Manage** → **Management Root**.
 - e) Select **Management** → **C** → **logout.html**
 - f) With the **logout.html** file highlighted, select **Manage** → **Export** to save the file.
2. Use an editor to open the logout.html file in the integration package.
3. Copy the script element in the HTML header (that is, the code contained by the script start and end tags):

```
<script language="Javascript">
.....
</script>
```

4. Open the existing logout.html file with an editor.
5. Paste the code from Step 3 above into the header tag.
6. Update the exception_list variable as described in the steps above.
7. In the body tag, add the parameter `delete_all_cookies('/', exception_list)`.
For example:

```
<body bgcolor="#FFFFFF" text="#000000" delete_all_cookies('/',  
exception_list)>
```

8. Save the modified logout.html.
9. Deploy the pending changes.
10. Restart the reverse proxy instance.

After configuring the logout page, proceed to [Chapter 3: Oracle PeopleSoft PeopleTools Configuration](#).

WebSEAL Configuration

It is recommended that Forms authentication is used so that single sign-out can be achieved with **PeopleSoft PeopleTools**. To enable Forms Authentication and disable Basic Authentication:

1. Stop the WebSEAL server.
2. Edit the <PDWEB_HOME>/etc/webseald-<instance-name>.conf file. For example: /opt/pdweb/etc/webseald-default.conf
3. Locate the **[forms]** stanza.
4. Update forms-auth to **https**.
5. Locate the **[ba]** stanza.
6. Update ba-auth to **none**.
7. Save the file.
8. Restart the WebSEAL instance.

Junction Creation

The selection of the most appropriate junctions for each environment is outside the scope of this integration. See the [IBM Security Access Manager Knowledge Center Junctions](#) page for details of each junction type.

The following example uses Transparent Path junctions to eliminate the requirement of path filtering. The Transparent Path junction name must exactly match the Context Root for PeopleSoft PeopleTools. For example, /psp.

For PeopleSoft, there are a number of root directories that will need to be accessed. These may differ depending on your PeopleSoft environment but at a minimum create transparent junctions for:

```
/psp  
/cs  
/ps
```

/psc

1. Using the **pdadmin** command-line utility, determine the WebSEAL server name. For example:

```
pdadmin sec_master> server list <instance-name>-webseald-  
<webseal-host-name>
```

2. Using the **pdadmin** command-line utility, create a Transparent Path to the **PeopleSoft PeopleTools** Gateway URL.

```
pdadmin sec_master> server task instance-webseald-server_name  
create -t tcp -c iv_user -h peoplesoft_fqdn -p port_no -v  
webseal_fqdn:port_no -x /psp
```

For example:

```
pdadmin sec_master> server task pt854-webseald-peopletools create  
-t tcp -c iv_user -h pt.ibm.com -p 443 -v webseal.ibm.com:443  
-x /psp
```

3. Create a transparent path junction for each of the PeopleTools application paths.

After creating the junctions, proceed to [WebSEAL Configuration Options](#).

WebSEAL Configuration Options

1. Edit the WebSEAL configuration file, located at <PDWEB_HOME>/etc/webseald-<instance-name>.conf.

For example: /opt/pdweb/etc/webseald-default.conf.

Modify the following entries:

Within the **[script-filtering]** stanza, enable the **script-filter** and **rewrite-absolute-with-absolute** parameters. For example:

```
[script-filtering]  
script-filter=yes  
...  
rewrite-absolute-with-absolute=yes
```

If the PeopleSoft application server hosts the PeopleSoft portal server, ensure that the WebSEAL authentication method and corresponding configuration will use HTTP cookies for session management. If WebSEAL is configured to use SSL, ensure that the **ssl-id-sessions** parameter is set to **no**:

```
[session]  
ssl-id-sessions = no
```

2. Save the file.
3. Restart the WebSEAL instance.

After modifying the WebSEAL Configuration Options, proceed to [Configuring the WebSEAL Logout Page](#).

Configuring the WebSEAL Logout Page

When a user successfully logs on to IBM Security Access Manager, and in turn through Single Sign-On (SSO) to PeopleTools, a session cookie from PeopleTools is stored in the browser's memory. Unless the user physically closes the browser, the session between the browser and PeopleTools remains open, even if the user has logged out of IBM Security Access Manager.

If another user were to re-use the same browser instance to log on to IBM Security Access Manager and access PeopleTools, PeopleTools may incorrectly identify the new user as the previous user due to the valid PeopleTools cookie.

To resolve this issue, the integration package includes a logout.html file, based on the default IBM Security Access Manager logout page. The supplied logout.html page includes JavaScript that invalidates session cookies from the browser upon logout from IBM Security Access Manager.

Note: WebSEAL returns the logout.html page when a user logs out using the pkmslogout function. This function is not available when WebSEAL has been configured to use the Basic Authentication (BA) authentication method. Hence this section is not relevant if WebSEAL is set to this mode.

To configure the WebSEAL logout page with the required JavaScript:

1. Make a backup copy of your existing logout page:
 - a) Locate the WebSEAL management page directory of your reverse proxy instance.
For example: /opt/pdweb/www-default/lib/html/C/
 - b) Backup the logout.html file.
2. Locate the logout.html file in the integration package.
3. Modify the logout.html file, updating the exception_list variable to include the list of cookies that you do not want destroyed:

```
// IBM Security Access Manager Integration
// for PeopleSoft
```



```
//
// Set this variable to a semi-colon list of the names of
// cookies you do not want to delete.
var exception_list = "";
```

4. Use this logout.html file to overwrite the existing logout.html file.
5. Restart the WebSEAL server.

If you have previously modified the default logout.html file, you can still add the required JavaScript functionality without abandoning your modifications. To do this:

1. Make a backup copy of your existing logout page:
 - a) Locate the WebSEAL management page directory of your reverse proxy instance.
For example: /opt/pdweb/www-default/lib/html/C/
 - a) Backup the logout.html file.
2. Use an editor to open the logout.html file in the integration package.
3. Copy the script element in the HTML header (that is, the code contained by the script start and end tags):

```
<script language="Javascript">
.....
</script>
```

4. Open the existing logout.html file with an editor.
5. Paste the code from Step 3 above into the header tag.
6. Update the exception_list variable as described in the steps above.
7. In the body tag, add the parameter delete_all_cookies('/', exception_list).
For example:


```
<body bgcolor="#FFFFFF" text="#000000" delete_all_cookies('/',
exception_list)>
```
8. Save the file.
9. Restart the WebSEAL instance.

After configuring the WebSEAL logout page, proceed to [Chapter 3: Oracle PeopleSoft PeopleTools Configuration](#).

Chapter 3: Oracle PeopleSoft PeopleTools Configuration

This section describes the integration steps required for Single Sign On between IBM Security Access Manager and PeopleTools.

After the following changes are applied, ensure that the PeopleTools application server and the Pure Internet Architecture server are restarted.

Creating a New User Profile

A new user profile (for example, `sso_default_user`) must be created within the PeopleTools database for an identity that the Web application server can use to authenticate to the PeopleTools application server. This user will be used to create a trust relationship between the PeopleTools Web content and the PeopleTools database.

To create the new user profile:

1. Log in to PeopleTools using a browser.
2. Click **Main Menu**, then select **PeopleTools** → **Security** → **User Profiles** → **User Profiles** and then select the **Add a New Value** tab.
3. Enter a User ID that will be used for public access to the PeopleTools application. For example, `sso_default_user`.
4. For the password, specify a long, random password that is hard to guess. Remember this password, as it will need to be used later in this integration process.
5. Select the **ID** tab. Select an **ID Type** of *None*.
6. The user should not belong to any roles. In fact, for security reasons, it is recommended that this user not have any roles or permissions.
7. Save the new user by clicking **Save**.
8. Ignore the **Symbolic ID missing** warning.
9. You will see a brief '*Saved*' message in the top-right corner of the page to indicate that the new user has been saved.

Note: This is not always obvious if using a horizontal scrollbar.

Update the PeopleTools Configuration

PeopleTools must be configured by editing the appropriate Web Profile.

1. Log into PeopleSoft using a browser.
2. Click **Main Menu**, then select **PeopleTools** → **Web Profile** → **Web Profile Configuration**.
3. Click the **Search** button.

4. Click the appropriate Web Profile (for example, PROD).
Note: To find the active Web Profile locate the `configuration.properties` file:
 - a) Navigate to


```
<PS_HOME>\weberv\<Web_Server>\applications\peoplesoft\
PORTAL.war\WEB-INF\psftdocs\<PIA_Name>\
```
 - b) Open the `configuration.properties` file in a text editor.
 - c) Locate the `WebProfile` entry.
5. On the **General** tab:
 - a) Uncheck **Compress Responses**,
 - b) Uncheck **Compress Response References**,
 - c) If this PeopleSoft application is not enrolled in PeopleSoft Single Sign-on, clear the **Authentication Domain** field. Otherwise, enter the appropriate **Authentication Domain** value.
 Refer to the PeopleSoft documentation for more information on PeopleSoft Single Sign-on.
6. On the **Security** tab:
 - a) In the **Public Users** section, select **Allow Public Access**. Enter the new User ID and password (created in the previous section) in the **User ID** and **Password** fields. For example, `sso_default_user`.
7. On the **Look and Feel** tab, perform the following steps to change the logout page from the default to a logout page that does not prompt for user ID and password:
 - a) In the **SignOn/Logout Pages** section, enter the name of the new logout page in the **Logout Page** field, overwriting the existing entries.
 For example,


```
logout_redirect.html, logout_redirect.html
```

Note: Without duplicating `logout_redirect.html`, a *500 internal server error* may be displayed when logging out of PeopleSoft.
 - b) Copy the `logout_redirect.html` page from the integration package to the appropriate directory.
 For example, on WebSphere Application Server:

```
<PS_APP_HOME>\installedApps\WebSphereNodeCell\
peoplesoft.ear\PORTAL.war\WEB-INF\psftdocs\ps
```

The new file contains sample code to redirect the user to the IBM Security Access Manager logout page. Ensure the user is redirected to the correct path by setting the Meta Refresh:

```
<meta http-equiv="refresh" content="0;
url=../../../../../pkmslogout">
```

For example:

```

<html>
  <head>
    <title>Logout Page</title>
    <meta http-equiv="refresh" content="0;
      url=../../../../../pkmslogout">
  </head>
  <body>
    <h1>Logout Page</h1>
    <p>You are being logged out.</p>
    <p>If you are not redirected in a few seconds <a
      href="../../../../../pkmslogout">click here</a>.</p>
  </body>
</html>

```

- c) Save the change to the web profile by clicking **Save**.

Create the SignOn PeopleCode

A sign-on function must be created for PeopleTools to retrieve the user ID from the HTTP request header passed by IBM Security Access Manager.

1. Open the Application Designer.
2. Choose **File** → **Open**.
3. Open a **Definition** of type *Record* and **Name** FUNCLIB_LDAP.
4. Choose **View** → **PeopleCode Display**.
5. In the displayed grid, double-click the checkbox at the junction of the **LDAPAUTH** row and the **FDe** column. This displays the PeopleCode functions.
6. At the end of the file, copy and paste the contents of `tivoliSSO.peoplecode`. This function reads the iv-user HTTP Request header passed by IBM Security Access Manager.
7. Locate the function called `getWWWAuthConfig()`. Set the default user ID to the name of the new user profile that you created earlier. For example:

```

Function getWWWAuthConfig()
  &defaultUserId = "sso_default_user";
End-Function;

```

8. Click **Save** to write the changes to the database.
9. Close the Application Designer.

Enable the SignOn PeopleCode

Perform the following steps to enable the sign-on function created above:

1. Login to PeopleSoft using a browser.
2. Click **Main Menu**, then select **PeopleTools** → **Security** → **Security Objects** → **Signon PeopleCode**.
3. Add a new row by clicking on the plus sign on the last row.
4. Enter data as follows:
 - a) The sequence number should be the next number after the ones already used.
 - b) The **Enabled** checkbox should be checked.
 - c) The **Record** field should be *FUNCLIB_LDAP*.
 - d) The **Field** name should be *LDAPAUTH*.
 - e) The **Event** name should be *FieldDefault*.
 - f) The **Function** name should be TivoliSSO, as defined in [Create the SignOn PeopleCode](#).
 - g) The **Exec Auth Fail** checkbox should remain unchecked. This PeopleCode should only run if the connection to the application server comes from a Web server that presents a valid user ID and password (that is, the new user ID and corresponding password specified in [Creating a New User Profile](#)).
4. Select the **Invoke As** radio button and enter the user name of the new user ID and corresponding password specified in [Creating a New User Profile](#). For example, `sso_default_user`.
Note: Ensure the new row that corresponds to the Tivoli SignOn PeopleCode is selected when this operation is performed.
5. Click the **Save** button.

Once activated the TivoliSSO PeopleCode is configured to output trace messages. Refer to [Configuring PeopleCode trace](#) for details on how to disable the trace.

Modify PeopleTools Session Expiration (Standard and Transparent Path WebSEAL Junctions)

The PeopleTools session expiration functionality must be modified when accessing PeopleTools applications via standard or transparent path IBM Security Access Manager junctions. PeopleTools generates a cookie to store the host name of the accessed PeopleTools application server. The PeopleTools session expiration JavaScript code checks that components of the URL being accessed match those of the PeopleTools cookie.

When the IBM Security Access Manager integration is applied using standard or transparent path junctions, the PeopleTools JavaScript code that checks for session validity fails and the user is redirected to the Session Expiration page.

To avoid this issue, PeopleTools must be made aware that the user's session is being maintained by IBM Security Access Manager. The PeopleTools JavaScript code checks the cookie to ensure that immediate redirection to the session expiration page does not occur.

Perform the following steps:

1. Open the Application Designer.
2. Choose **File → Open**.
3. Select a **Definition** of type *HTML* and **Name** PT_SAVEWARNINGSRIPT. If you are only permitted to open the record for read-only purposes, refer to the note at the bottom of this section for details on how to modify the access permission.
4. Add the following code to the end of the file:

```
//% IBM Security Access Manager Integration
//% Check for WebSEAL junction cookie presence
function isViaWebSEAL(cookieList)
{
    if((cookieList == null) || (cookieList == ""))
        return false;

    if((cookieList.indexOf('PD-H-SESSION-ID=') != -1) ||
        (cookieList.indexOf('PD-S-SESSION-ID=') != -1))
    {
        return true;
    }

    return false;
}
```

5. Locate the **getLoginCookieValue** method, and update the code as follows:

ORIGINAL LINE OF CODE

```
if((urlpath.indexOf(winurlpath) != -1) && urlpath.length ==
winurlpath.length && (winhref.indexOf(pshome) != -1))
```

should be replaced with:

NEW LINE OF CODE

```
if((urlpath.indexOf(winurlpath) != -1) && urlpath.length ==
winurlpath.length && (winhref.indexOf(pshome) != -1) ||
(isViaWebSEAL(allcookies)))
```

6. Choose **File → Save**.
7. Choose **File → Exit**.

Note: If you can only open the file in read-only mode, you may require additional privileges to modify the JavaScript as described above. To grant the required permission,

perform the following steps:

1. Open the Application Designer.
2. Choose **Go** → **Definition Security**. A new window is displayed.
3. Choose **File** → **Open** → **Permission Lists**.
4. Select ALLPAGES for FDM, or HCPPALL for HR.
5. Move PEOPLETOOLS from the right pane to the left pane and ensure the **Display Only** is set to *No*.
If PEOPLETOOLS is already on the left and **Display Only** is set to *Yes*, move PEOPLETOOLS to the right and then back to the left as above.
6. Choose **File** → **Save**.
7. Choose **File** → **Exit**.
8. Backup the **expire.html** and **expire.wml** files found in
<PS_APP_HOME>\installedApps\WebSphereNodeCell\peoplesoft.ear\
PORTAL.war\WEB-INF\psftdocs\ps when using IBM WebSphere.
9. Modify all the lines that contain **cmd=login** to **cmd=start**.

Restart Application Servers

Restart the Application Servers as follows:

1. Stop the PeopleSoft domain by using the **psadmin** utility:
 - a) Open a command prompt.
 - b) Execute **psadmin**.
 - c) Enter **1** for **Application Server**.
 - d) Enter **1** for **Administer a Domain**.
 - e) Enter the number of the desired domain.
 - f) Enter **2** for **Domain shutdown menu**.
 - g) Enter **1** for **Normal shutdown**.
2. Remove all files within the Web application server cache. For example, on WebSphere Application Server:

```
<PS_APP_HOME>\installedApps\WebSphereNodeCell\peoplesoft.ear\  
PORTAL.war\ps\cache
```

3. Start the PeopleSoft domain by using the **psadmin** utility.
 - a) Open a command prompt.
 - b) Execute **psadmin**.
 - c) Enter **1** for **Application Server**.
 - d) Enter **1** for **Administer a Domain**.
 - e) Enter the number of the desired domain.
 - f) Enter **1** for **Boot this domain**.

Enter **1** for **Boot (Serial Boot)**.

4. Restart the web application server.

Updating PeopleSoft PeopleTools Launch URLs

After completing the integration all links used to navigate to any application served by PeopleTools must be updated to reflect the `cmd=start` parameter. This includes bookmarks, shortcuts, or portal launch pages and must be set to ensure that the custom PeopleCode is called.

The IBM Security Access Manager HTTP Transformation Rule feature may be used to automatically modify requests to `cmd=login` with `cmd=start`.

Refer to the [*IBM Security Access Manager Knowledge Center HTTP transformations*](#) page for details on applying HTTP transformations to modify the URI in the HTTPRequest.

Validating the Integration

To confirm that your IBM Security Access Manager integration with PeopleSoft PeopleTools has been successfully configured:

1. Open a browser and access the PeopleSoft application with the following URL:

WebSEAL with Standard Junction

`https://webseal_host_fqdn/junction_name/psp/ps/?cmd=start`

WebSEAL with Transparent Path Junction

`https://webseal_host_fqdn/psp/ps/?cmd=start`

WebSEAL with Virtual Host Junction

`https://peoplesoft_host_fqdn/psp/ps/?cmd=start`

2. Authenticate to IBM Security Access Manager with a user that has been provisioned in PeopleSoft.
3. Upon successful authentication, the PeopleSoft application main page should be displayed.

Removing the Integration

The uninstall process is virtually a reverse of the installation process described above. To remove the integration, you only need to restore your original PeopleSoft settings.

If you plan to modify your network settings and re-deploy WebSEAL, you may also wish to restore your original WebSEAL settings.

Chapter 4: Troubleshooting

If you experience any problems during integration, examine the following notes for help in identifying problems.

Collecting Support Data

This section describes the specific MustGather data needed for problem determination for Oracle PeopleSoft PeopleTools integration issues.

The following integration specific files should be gathered along with the relevant IBM Security Access Manager data (see the [IBM Security Access Manager MustGather page](#)) and submitted to support to aid in problem determination:

- The TivoliSSO PeopleCode trace file, specified in the TivoliSSO function as `c:\temp\tivoli_sso_peoplecode.log`. See Step 4 of [Create the SignOn PeopleCode](#).
- The configuration file which lists the active Web Profile, located in `<PS_APP_HOME>\installedApps\WebSphereNodeCell\peoplesoft.ear\PORTAL.war\WEB-INF\psftdocs\<PIA_Name>\configuration.properties`

Configuring PeopleCode trace

Tracing in the custom PeopleCode should be used to aid in debugging authentication errors and should not be left enabled in a production environment due to the volume of messages and unmanaged, simple flat file format.

TivoliSSO PeopleCode trace overview

The trace file location is specified at the start of the `tivoliSSO()` function. The first parameter passed to the `GetFile` function is the absolute filepath of the log file.

This must be updated for the operating system where PeopleSoft is installed.

For example:

- Windows systems: `C:\temp\tivoli_sso_peoplecode.log`

```
&traceFile = GetFile("c:\temp\tivoli_sso_peoplecode.log", "A",  
%FilePath_Absolute);
```

- **UNIX systems:** /tmp/tivoli_sso_peoplecode.log
`&traceFile = GetFile("/tmp/tivoli_sso_peoplecode.log", "A",
 %FilePath_Absolute);`

The following syntax is used to ensure that the file has been successfully opened before attempting to log a trace message:

```
If &traceFile.Isopen Then
    &traceFile.Writeline("INFO:TivoliSSO()entry.");
End-If;
```

The if statement ensures the file is open before attempting to write the message INFO:TivoliSSO()entry. This logic should always be used when logging messages to avoid any possible exceptions.

Disabling TivoliSSO PeopleCode trace

To disable tracing, comment out each of the `If &traceFile.Isopen Then` statements as well as the `&traceFile = GetFile()` line.

For example:

```
Function TivoliSSO()
    /*&traceFile = GetFile("c:\temp\tivoli_sso_peoplecode.log", "A",
    %FilePath_Absolute);*/
    ...
    /*If &traceFile.Isopen Then
        &traceFile.Writeline("INFO:TivoliSSO()entry.");
    End-If;*/
    ...
    If %PSAuthResult = True And
        &authMethod <> "LDAP" And
        &authMethod <> "SSO" Then
        /*If &traceFile.Isopen Then
            &traceFile.Writeline("INFO:PSAuthResult and authMethod OK.");
        End-If;*/
    ...
    ...
```

Minimal or incomplete user options

If the user's options are minimal or incomplete after authenticating, it is likely that an error has been encountered with the new PeopleCode function. Check its log file for more information on where the failure occurred. Common problems include:

- Forgetting to set the `defaultUserId` value in the `getWWWAuthConfig()` PeopleCode function. For more information, see [Create the SignOn PeopleCode](#).
- Forgetting to enable the PeopleCode. For more information, see [Enable the SignOn PeopleCode](#).

If absolute URLs embedded in scripts are not displaying correctly, ensure that you have enabled the `script-filter` and `rewrite-absolute-with-absolute` parameters. See the instructions in [Web Reverse Proxy Configuration Options](#) or [WebSEAL Configuration Options](#).

Also, ensure you have created your Standard or Transparent Path Junctions with the `-v` option. See the instructions in the [Web Reverse Proxy Configuration](#) or [WebSEAL Configuration](#).

Logged warnings

It is normal after successful Single Sign-On to see warning lines in the log file. These are for subsequent requests after Single Sign-On has been achieved, where transactions are being processed for authenticated users. Such warnings can be ignored. It may be advisable to remove these trace messages from the PeopleCode to avoid confusion with system administrators in a production environment. For example, the following trace is an extract from a successful Single Sign-On. Note that there are multiple calls to the `TivoliSSO()` function in this case.

```
INFO: TivoliSSO() entry.
INFO: PSAuthResult and authMethod OK.
INFO: after getWWWAuthConfig().
sso_default_user
INFO: %SignonUserId = &defaultUserId
INFO: userID is valid.
PS
INFO: TivoliSSO() exit.
INFO: TivoliSSO() entry.
INFO: PSAuthResult and authMethod OK.
INFO: after getWWWAuthConfig().
sso_default_user
WARNING: (%SignonUserId = &defaultUserId). This could be normal
if not the first invocation of a user session.
```

```

PS
sso_default_user
INFO: TivoliSSO() exit.
INFO: TivoliSSO() entry.
INFO: PSAuthResult and authMethod OK.
INFO: after getWWWAuthConfig().
sso_default_user
WARNING: (%SignonUserId = &defaultUserId). This could be normal
if not the first invocation of a user session.
PS
sso_default_user
INFO: TivoliSSO() exit.
INFO: TivoliSSO() entry.
INFO: PSAuthResult and authMethod OK.
INFO: after getWWWAuthConfig().
sso_default_user
WARNING: (%SignonUserId = &defaultUserId). This could be normal
if not the first invocation of a user session.
PS
sso_default_user
INFO: TivoliSSO() exit.

```

Problems creating user profile

When creating a new user profile in the PeopleSoft database (as described in [Creating a New User Profile](#)), a problem has been seen where the user initially needs to be added to the Guest role, but can later be removed after Single Sign-On has been achieved at least once.

Problems related to the log in or log off process

The following notes describe some common problems related to the log in or log out of process.

- If the server returns an error such as *500 internal server error* when logging off PeopleTools, check that the logout.html text was entered twice (that is `logout.html, logout.html`) in the Logout Page field, as described in [Update the PeopleTools Configuration](#).
- If the login page is displayed after signing in to IBM Security Access Manager, ensure that you are specifying the correct command in the URL. For example, specify `?cmd=start` at the end of the URL, rather than `?cmd=login`. Also ensure that you are not using the PeopleTools default signoff.html page.
- If the browser performs multiple, apparently infinite redirects to WebSEAL and the PeopleTools server after a successful WebSEAL login, it is likely that the PeopleTools session expiration has not been configured correctly. Ensure that the

instructions provided in [Modify PeopleTools Session Expiration \(Standard and Transparent Path WebSEAL Junctions\)](#) have been implemented correctly.

- If a user isn't signed in as expected, ensure that both IBM Security Access Manager and PeopleTools usernames match in case. Usernames are case insensitive in IBM Security Access Manager and case sensitive in PeopleSoft PeopleTools.

PeopleTools inactivity warning

The PeopleTools inactivity warning value should be set to less than the value of the WebSEAL session timeout. This configuration allows the PeopleTools inactivity prompt to be displayed and run successfully.

You can configure the WebSEAL session timeout using the **timeout** and **inactive-timeout** entries of the **[session]** stanza in the WebSEAL configuration file.

Perform the following steps to configure the PeopleTools inactivity warning value:

1. Log into PeopleTools using a browser.
2. From the menu, select **PeopleTools > Web Profile > Web Profile Configuration**.
3. Click **Search**.
4. Click the appropriate Web Profile (for example, PROD).
Note: To find the active Web Profile locate the configuration.properties file:
 - I. Navigate to <PS_HOME>\webseal\<Web_Server>\applications\peoplesoft\PORTAL.war\WEB-INF\psftdocs\<PIA_Name>
 - II. Open the configuration.properties file in a text editor.
 - III. Locate the WebProfile entry.
5. On the Security tab:
 - I. Update the **Inactivity Warning** field to use a value smaller than the WebSEAL session or inactivity timeout.
 - II. Click **Save**.
6. Restart the Application Servers as follows:
 - I. Stop the PeopleTools domain by using the **psadmin** utility.
 - II. PeopleTools domain using the **psadmin** utility.
 - III. Restart the Web application server.

Filtering the 'text/plain' HTTP Content-Type

In some situations, PeopleTools HTTP responses are returned to WebSEAL with the **Content-Type** header set to text/plain. By default, WebSEAL does not filter responses of this type, which results in broken links.

This problem can be resolved by either:

- Setting the default **Content-Type** in the Web server hosting PeopleTools to text/html. The method for setting this value depends on the Web server being used. Consult your Web server documentation for more information.

Or

- Adding text/plain to the **filter-content-types** stanza of the WebSEAL configuration file:

```
[filter-content-types]
type = text/plain
```

HttpOnly Cookies

For added security, WebSEAL supports setting the **HttpOnly** option on the WebSEAL cookies that are returned to the browser. Any cookie that has the **HttpOnly** option set prevents client-side JavaScript from accessing the cookie.

PeopleTools uses JavaScript to manage user session expiration. The **isViaWebSEAL** JavaScript function provided with this integration manages the WebSEAL user sessions in conjunction with the PeopleTools session expiration JavaScript. See [Modify PeopleTools Session Expiration \(Standard and Transparent Path WebSEAL Junctions\)](#) for more information.

The **isViaWebSEAL** JavaScript function requires access to the WebSEAL cookies. If the **HttpOnly** option is set on these cookies, the **isViaWebSEAL** JavaScript fails to find the WebSEAL session cookies and the PeopleTools session expiry page is displayed after a successful log on to WebSEAL.

This problem results from the **isViaWebSEAL()** function searching for the **PD-H-SESSION-ID** or **PD-S-SESSION-ID** cookies:

```
//% IBM Security Access Manager Integration
//% Check for IBM Security Access Manager WebSEAL cookie presence
function isViaWebSEAL(cookieList)
{
    if((cookieList == null) || (cookieList == ""))
        return false;

    if((cookieList.indexOf('PD-H-SESSION-ID=') != -1) ||
        (cookieList.indexOf('PD-S-SESSION-ID=') != -1))
    {
        return true;
    }

    return false;
}
```

When the **use-http-only-cookies** flag has been set in WebSEAL, neither of these cookies can be found.

If you need to use the **HttpOnly** cookie option in your environment, you can modify the **isViaWebSEAL** function to always return true.

To make this change, perform the following steps:

1. Open the Application Designer.
2. Choose **File** → **Open**.
3. Select a **Definition** of type *HTML* and **Name** PT_SAVEWARNINGSRIPT. If you are only permitted to open the record for read-only purposes, refer to the note at the bottom of [Modify PeopleTools Session Expiration \(Standard and Transparent Path WebSEAL Junctions\)](#) for details on how to modify the access permission.
4. Update the **isViaWebSEAL** function at the end of the file to be:

```
//% IBM Security Access Manager Integration
//% Check for IBM Security Access Manager WebSEAL cookie presence
function isViaWebSEAL(cookieList)
{
    return true;
}
```

5. Choose **File** → **Save**.
6. Choose **File** → **Exit**.

Notices

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 character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, 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 might 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
2Z4A/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 document 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 measurement 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 cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. ©Copyright IBM Corp. _enter the year or years_. All rights reserved.

If you are viewing this information in softcopy form, the photographs and color illustrations might not be displayed.

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at Copyright and trademark information; at www.ibm.com/legal/copytrade.shtml.

Adobe, Acrobat, PostScript and all Adobe-based trademarks are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

UNIX is a registered trademark of The Open Group in the United States and other countries.



Java™ and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

Other company, product, and service names may be trademarks or service marks of others.