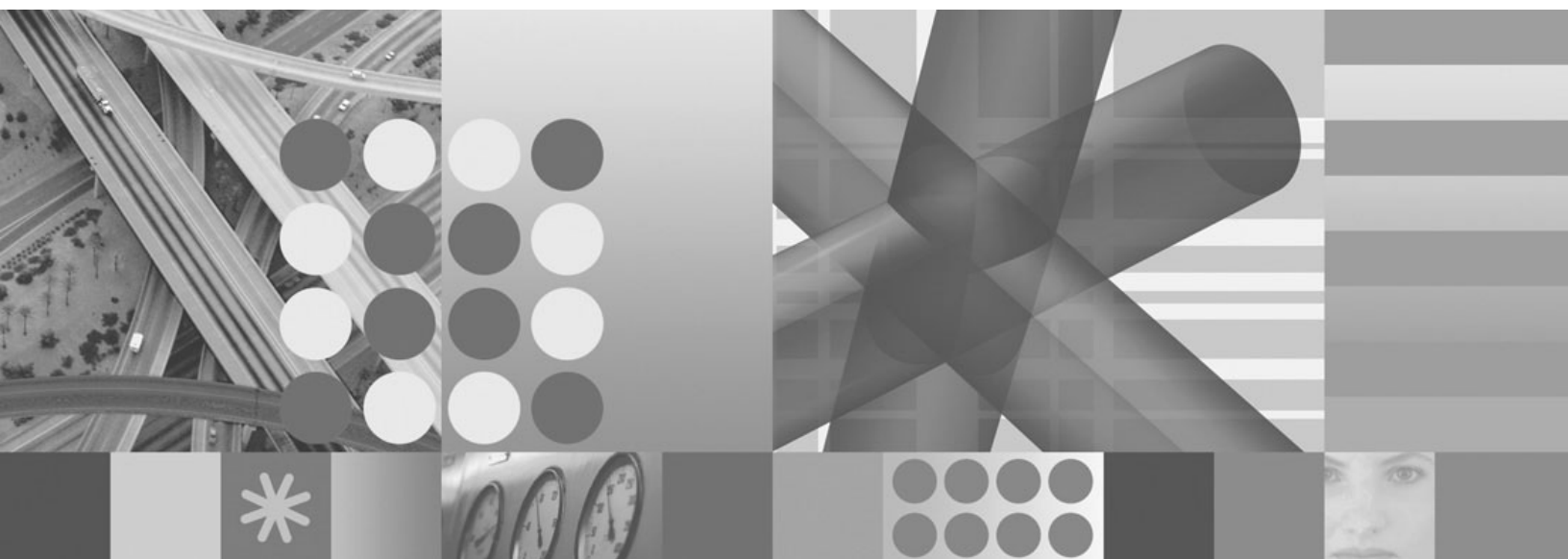




**PeopleSoft PeopleTools 8.4
Integration Guide**



**PeopleSoft PeopleTools 8.4
Integration Guide**

Note

Before using this information and the product it supports, read the information in Appendix B, “Notices,” on page 25

This edition applies to version 3.0.05 of the Tivoli Access Manager integration with PeopleSoft PeopleTools 8.4, and to all subsequent releases and modifications until otherwise indicated in new editions. This edition replaces previous editions for earlier versions.

© **Copyright International Business Machines Corporation 2004, 2008.**

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

Contents

Preface	v
Who Should Read This Guide	v
Contacting Software Support	v
Tivoli technical training	v
Conventions Used in this Book	vi
 Chapter 1. Introducing Tivoli Access Manager Integration with PeopleSoft PeopleTools	 1
Introduction	1
Using the Tivoli Access Manager Plug-in for Web Servers	1
Using Tivoli Access Manager WebSEAL	2
Integration Product Version Information	3
Integration Package Contents	3
Integration Checklist	4
Integration Process Flow	5
 Chapter 2. Integration Steps	 7
Before you Start	7
Configuring the Web Plug-in	7
Web Plug-in Configuration Options	7
Configuring the Web Plug-in Logout Page	8
Configuring Tivoli Access Manager WebSEAL	9
Creating a WebSEAL Junction	9
WebSEAL Configuration Options	11
Configuring the WebSEAL Logout page	12
PeopleTools Configuration	13
Create a New User Profile	13
Update the PeopleTools Configuration	13
Create the SignOn PeopleCode	14
Enable SignOn to PeopleCode	15
Remove PeopleSoft Inactivity Timeout	15
Restart Application Servers	16
Checking the Integration	17
Uninstallation	17
 Chapter 3. Troubleshooting	 19
 Appendix A. Support information	 21
Searching knowledge bases	21
Search the information center on your local system or network	21
Search the Internet	21
Obtaining fixes	21
Contacting IBM Software Support	22
Determine the business impact of your problem	23
Describe your problem and gather background information	23
Submit your problem to IBM Software Support	23
 Appendix B. Notices	 25
Trademarks	26

Preface

This guide tells you how to configure and manage your IBM® Tivoli® Access Manager installation to work with PeopleSoft PeopleTools to achieve Single Sign-On (SSO) capability.

This document assumes there is a Tivoli Access Manager environment installed, configured and running on your network. It also assumes that the PeopleSoft application server is installed, configured and running. This guide does not provide details on the installation and administration of these products, except where necessary to achieve integration.

Who Should Read This Guide

This guide is for those responsible for the installation, deployment and administration of Tivoli Access Manager and PeopleSoft. The reader should be familiar with the administration of Tivoli Access Manager, Tivoli Access Manager WebSEAL and PeopleSoft products including PeopleCode.

Readers should also be familiar with the following:

- PC and UNIX® operating systems,
- Internet protocols, including HTTP, SSL, HTTPS, HTML and TCP/IP,
- Lightweight Directory Access Protocol (LDAP) and directory services,
- A supported user registry,
- Security management,
- Authentication and authorization.

Contacting Software Support

Contact IBM Software Support by using the methods described in the *IBM Software Support Guide* at the following Web site:

<http://techsupport.services.ibm.com/guides/handbook.html>

The guide provides the following information:

- Registration and eligibility requirements for receiving support
- Telephone numbers, depending on the country in which you are located
- A list of information you should gather before contacting customer support

For more information, see “Contacting IBM Software Support” on page 22.

Tivoli technical training

For Tivoli technical training information, refer to the IBM Tivoli Education Web site: <http://www.ibm.com/software/tivoli/education>.

Conventions Used in this Book

The following typeface conventions are used in this book:

Bold Lowercase commands or mixed case commands that are difficult to distinguish from surrounding text, keywords, parameters, options, names of Java™ classes, and objects are in **bold**.

Italic Variables, titles of publications, and special words or phrases that are emphasized are in *italic*.

Monospace

Code examples, command lines, screen output, file and directory names that are difficult to distinguish from surrounding text, system messages, text that the user must type, and values for arguments or command options are in monospace.

Chapter 1. Introducing Tivoli Access Manager Integration with PeopleSoft PeopleTools

This chapter has the following sections:

- “Introduction”
- “Integration Product Version Information” on page 3
- “Integration Package Contents” on page 3
- “Integration Checklist” on page 4
- “Integration Process Flow” on page 5

Introduction

This integration guide describes the procedures for integrating the IBM Tivoli Access Manager for e-business with PeopleSoft PeopleTools to achieve Single Sign-On (SSO) capability.

Integration can be achieved using either the Tivoli Access Manager Plug-in for Web Servers or Tivoli Access Manager WebSEAL. Read the following sections carefully to select the scenario that best fits your corporate environment and network architecture.

Using the Tivoli Access Manager Plug-in for Web Servers

This integration provides Single Sign-On (SSO) between Tivoli Access Manager and PeopleSoft by deploying Tivoli Access Manager Plug-in for Web Servers, which intercepts requests, authenticating and authorizing user access to PeopleSoft.

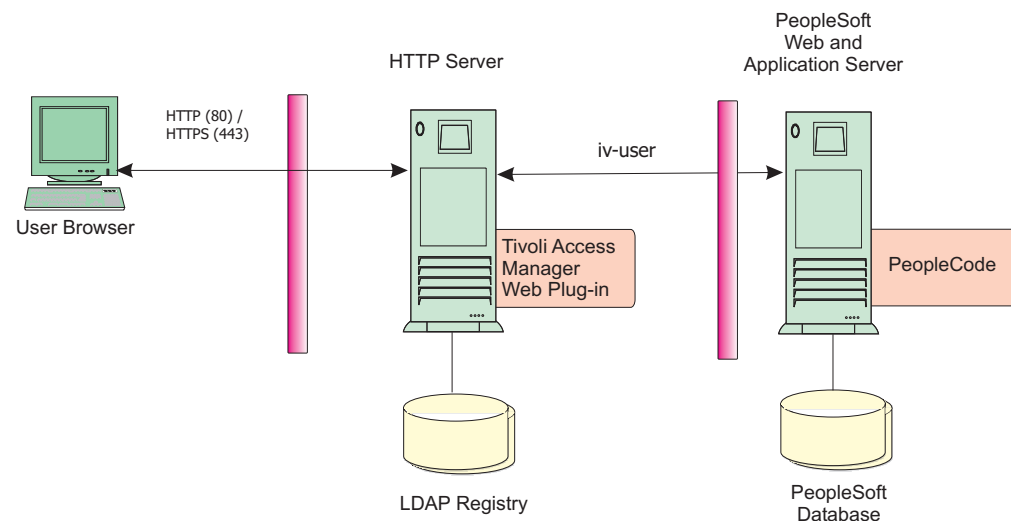


Figure 1. Architecture of the Tivoli Access Manager integration with PeopleSoft using Tivoli Access Manager Plug-in for Web Servers.

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

1. A Client accesses PeopleSoft through their Web browser.
2. Web Plug-in intercepts the request, authenticates and authorizes the user.

3. On successful authentication, Web plug-in creates and inserts an HTTP header into the request that contains the authenticated username.
4. The PeopleSoft Application Server is configured to accept and trust the user ID inserted by Web Plug-in, using PeopleSoft PeopleCode.
5. The PeopleSoft Application Server logs in the user and grants user access.

Using Tivoli Access Manager WebSEAL

This integration provides Single Sign-On (SSO) between Tivoli Access Manager and PeopleSoft PeopleTools by deploying WebSEAL as a reverse-proxy server in the front of the PeopleSoft Web Application Server. WebSEAL acts as a security gateway between the client browser and the PeopleSoft Web Application Server, where it authenticates and authorizes users attempting to access the PeopleSoft applications. PeopleTools must be configured to accept the external authentication performed by the third-party server (WebSEAL, in this case).

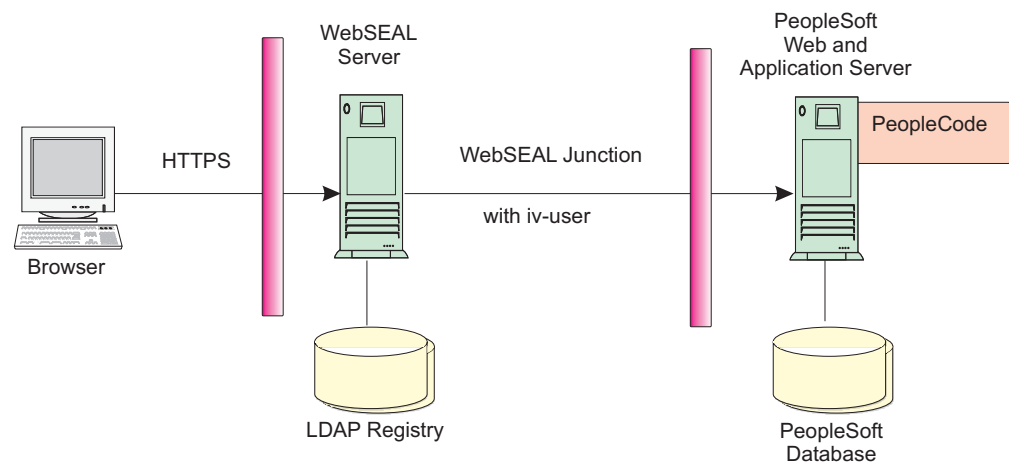


Figure 2. Component architecture of the Tivoli Access Manager integration with PeopleSoft using Tivoli Access Manager WebSEAL.

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

1. A client accesses PeopleSoft applications through WebSEAL.
2. WebSEAL intercepts the request, authenticates and authorizes the user.
3. On successful authentication, WebSEAL passes the request to the PeopleSoft application, together with the authenticated user ID as part of the HTTP header.
4. PeopleTools is configured to accept and trust this user ID from WebSEAL using PeopleSoft PeopleCode.
5. The PeopleTools Application Server logs in the user and grants user access.

Integration Product Version Information

The integration scenarios detailed in this document are for the following product versions:

- PeopleSoft applications using PeopleTools 8.45 to 8.49
- Either:
 - IBM Tivoli Access Manager Base 5.1, and
 - IBM Tivoli Access Manager Plug-in for Web Servers 5.1
- Or:
 - IBM Tivoli Access Manager Base 5.1, and
 - IBM Tivoli Access Manager WebSEAL 5.1

Integration Package Contents

The integration package contains the following files:

File Name	Description
am_peoplesoft_int_guide.pdf	This document.
tivoliSS0.peoplecode	Sample code provided for the tivoliSS0() function.
isViaWebSEAL.javascript	Sample code provided to update the PT_SAVEWARNINGSCRIPT definition.
logout.html	Used by WebSEAL upon user logout. It releases cookies within the user browser.
logout_redirect.html	Sample logout page used by PeopleSoft to provide a redirect link to the WebSEAL or Web Plug-in logout page.

Integration Checklist

The following tables can be printed and used as a checklist to assist you as you work through the integration process. A list of each major task heading is provided, with a check box next to it. Each task is detailed fully in the following sections.

Fill out the **Planning** column prior to starting the integration. Once all steps for the heading are complete, return to this page and check the appropriate box in the **Completed** column.

Table 1. Tivoli Access Manager Plug-in For Web Servers Configuration

Planning	Completed	Task Heading
☐ To Do ☐ N/A	☐ Done	Web Plug-in Configuration Options
☐ To Do ☐ N/A	☐ Done	Configuring the Web Plug-in Logout Page

Table 2. Tivoli Access Manager WebSEAL Configuration

Planning	Completed	Task Heading
☐ To Do ☐ N/A	☐ Done	Creating a junction: • Virtual host junction • Transparent path junction • Standard junction
☐ To Do ☐ N/A	☐ Done	WebSEAL Configuration Options
☐ To Do ☐ N/A	☐ Done	Configuring the WebSEAL Logout Page

Table 3. PeopleSoft Configuration

Planning	Completed	Task Heading
✓ To Do	☐ Done	Create a New User Profile
✓ To Do	☐ Done	Update the PeopleTools Configuration
✓ To Do	☐ Done	Create the SignOn PeopleCode
✓ To Do	☐ Done	Enable SignOn to PeopleCode
☐ To Do ☐ N/A	☐ Done	Remove PeopleSoft Inactivity Timeout
✓ To Do	☐ Done	Restart the Application Servers

Integration Process Flow

The diagram below illustrates the process of integration procedures (as described in this document) required to achieve integration.



Figure 3.

Chapter 2. Integration Steps

This chapter includes the following sections:

- “Before you Start”
- “Configuring the Web Plug-in”
- “Configuring Tivoli Access Manager WebSEAL” on page 9
- “PeopleTools Configuration” on page 13
- “Checking the Integration” on page 17
- “Uninstallation” on page 17

Before you Start

Before you start:

- Read the scenario options described in “Introduction” on page 1. Determine the option best suited to your environment.
- Check the software prerequisites described in “Integration Product Version Information” on page 3.
- Determine the procedures that you will need to follow by referring to the integration flowchart provided in “Integration Process Flow” on page 5.
- Then print out the tables provided in “Integration Checklist” on page 4. These will help you work your way through this guide.

Before beginning the integration, you should also be aware of the following:

- Users must have an account in Tivoli Access Manager as well as a corresponding account in the PeopleSoft user registry. The username in Tivoli Access Manager must match the account name for the corresponding user in the PeopleSoft user registry for mapping between the directories.

Configuring the Web Plug-in

This section describes the integration steps required on Web Plug-in. The Tivoli Access Manager Plug-in for Web Servers must be restarted after these changes have been made.

Web Plug-in Configuration Options

Configure the Web Plug-in to generate the `iv-user` and `iv-user-1` HTTP headers:

1. Open `pdwebpi.conf`.
2. In the `[common modules]` stanza, set the `post-authzn` value to `iv-headers`:

```
[common modules]
...
post-authzn=iv-headers
```
3. In the `[iv-headers]` stanza, set the `generate` value to `iv-user`, `iv-user-1`:

```
[iv-headers]
...
generate=iv-user, iv-user-1
```
4. Save and close the file.

For details of Web Plug-in HTTP header creation, refer to the *Tivoli Access Manager Plug-in for Web Servers Integration Guide*, specifically the section *Configuring single sign-on to secure applications using HTTP headers*.

Configuring the Web Plug-in Logout Page

Whenever a user successfully logs on to the Web Plug-in, and in turn through Single Sign-on (SSO) to PeopleSoft, a session cookie from PeopleSoft is stored in the browser's memory. Unless the user physically closes the browser, the session between the browser and PeopleSoft remains open, even if the user has logged out of Tivoli Access Manager. If another user were to re-use the same browser window to log on to the Web Plug-in and access PeopleSoft, PeopleSoft might assume that the new user was the same as the previous user.

To solve this problem, the integration package includes a `logout.html` file, similar to the `logout.html` file that is supplied with the default the Web Plug-in installation. The supplied `logout.html` page includes JavaScript™ that erases session cookies from the browser upon logout from the Web Plug-in.

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

To configure the Web Plug-in logout page with the required JavaScript:

1. Make a backup copy of your existing logout page:
`webpi_install_dir\nls\html\locale\logout_success.html`
2. Locate the `logout.html` file in the integration package. Change the name of the file to `logout_success.html`.
3. Use this `logout_success.html` file to overwrite the existing `logout_success.html` file.
4. Modify the `logout_success.html` file, updating the **exception_list** variable to include the list of cookies that you do not want destroyed.

```
// IBM Tivoli 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 = "";
```
5. Restart the Web Plug-in server.

If you have previously modified the default `logout_success.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_success.html` file in the directory:
`webpi_install_dir\nls\html\locale\logout_success.html`
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_success.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 step 4 at the beginning of this section.
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 Web Plug-in server.

Configuring Tivoli Access Manager WebSEAL

This section describes the integration steps required on WebSEAL. After you have performed the following steps, WebSEAL must be restarted for the changes to be applied.

Creating a WebSEAL Junction

A WebSEAL junction must be created to connect WebSEAL with the PeopleSoft PeopleTools Server. The WebSEAL junction can be configured to use either TCP or SSL (recommended).

The junction creation command must specify the `-c iv_user,iv_user_l` option, which configures WebSEAL to send the authenticated username in the `iv-user` HTTP header and the user's DN in the `iv-user-l` HTTP header. The user's DN is only required when PeopleSoft is synchronized with an LDAP server. Refer to the PeopleSoft documentation for more details.

There are three types of junction that can be created to achieve this integration:

- Virtual host junction,
- Transparent path junction, or
- Standard junction.

The details for creating such junctions are detailed in the sections that follow.

For complete details on WebSEAL junction creation, refer to the *IBM Tivoli Access Manager WebSEAL Administration Guide*.

Virtual host junction

WebSEAL supports virtual hosting. The use of virtual host junctions eliminates the limitations of URL filtering. Virtual host junctions allow WebSEAL to communicate with local or remote virtual hosts. WebSEAL uses the HTTP Host header in client requests to direct those requests to the appropriate document spaces located on junctioned servers or on the local machine.

Local DNS's will need to be updated so that references to the PeopleSoft PeopleTools Server will actually reference the WebSEAL server.

Virtual hosting introduces some DNS and session management challenges. For details, refer to the *Tivoli Access Manager WebSEAL Administration Guide*.

To create the Virtual host junction (example command, entered as one line):

```
pdadmin> server task instance-webseald-server_name virtualhost create -t tcp
-h peoplesoft_fqdn -p port_no -c iv_user junction_name
```

Refer to the *Tivoli Access Manager WebSEAL Administration Guide* for more details on Virtual Host junctions.

Virtual hosting requires that the port number is the same from Client to WebSEAL as it is from WebSEAL to the backend (PeopleSoft) server.

So if the path to access PeopleSoft directly is `http://peoplesoft_fqdn:port_no/path`, then this port (*port_no*) must also be listening on the WebSEAL Server.

To ensure that this is the case, either:

- Configure WebSEAL to listen to this port as its default port, or
- Add this port to the [interfaces] stanza of the WebSEAL configuration file as follows:
 1. Open the file `WebSEAL_Install_Dir/etc/instance-webseald.conf`.
 2. In the [interfaces] stanza add the following (for a http port):
`interface_name = http-port= port_no`

You can then access WebSEAL at `http://webseal.com:port_no`.

Refer to the *Tivoli Access Manager WebSEAL Administration Guide* for more details on creating interfaces.

After creating a virtual host junction as described above, proceed to “Configuring the WebSEAL Logout page” on page 12.

Transparent path junction

Links to resources located on the backend server must be filtered by WebSEAL to ensure that the user does not access it directly but rather through the WebSEAL junction. There are three sections of a URL that need to be considered:

- Protocol (http/https)
- Hostname:port
- Path

The Transparent Path junction removes the need to filter the path.

A transparent path junction observes a crucial requirement: the configured junction name must match the name of a subdirectory under the root of the back-end server document space. All resources accessed through this junction must be located under this subdirectory. The transparent path junction name represents the name of the actual subdirectory on the back-end server.

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 you will need junctions to the following:

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

Create a transparent path junction to each of the above directories.

To create a transparent path junction, use the same command as for creating a standard junction but include the `-x` option. For details on creating a standard junction, refer to “Standard junction” on page 11.

Example command (entered as one line):

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

For more details on transparent path junctions, refer to the *Tivoli Access Manager WebSEAL Administration Guide*.

After creating a transparent path junction as described above, proceed to “WebSEAL Configuration Options.”

Standard junction

A WebSEAL junction is required to connect WebSEAL to the PeopleSoft application server. The junction can be setup to use either SSL (recommended) or TCP protocol. For details of WebSEAL junction creation, refer to the *IBM Tivoli Access Manager WebSEAL Administration Guide*.

In addition to the standard procedures for junction creation, this integration requires the following parameters:

1. Specify the `-c iv_user` flag to allow WebSEAL to pass the user ID to PeopleSoft in the form of a HTTP header.
2. Ensure that the host name supplied with the `-h` parameter is the fully-qualified DNS name (FQDN) of the PeopleSoft application server machine.
3. If the PeopleSoft application server is running on a non-default HTTP port, add the `-v fqdn:port` parameter. This must only be used for non-default HTTP ports (that is, not for port 80).

Example command for a standard junction (entered as one line):

```
pdadmin> server task instance-webseald-server_name create -t tcp  
-h peoplesoft_fqdn -p port_no -c iv_user /junction_name
```

Note: When using an SSL junction, ensure that browsers access WebSEAL using HTTPS, rather than HTTP. Browsers accessing WebSEAL using HTTP will experience issues related to incorrect filtering by WebSEAL.

For more detailed instructions on WebSEAL junction creation, refer to the *IBM Tivoli Access Manager WebSEAL Administration Guide*.

After creating a Standard junction as described above, proceed to “WebSEAL Configuration Options.”

WebSEAL Configuration Options

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, check the `WebSEAL_install_dir/etc/instance-webseald.conf` file and ensure that the **ssl-id-sessions** parameter is set to `no`:

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

Restart WebSEAL for the above changes to take effect.

After configuring WebSEAL as described above, proceed to “Configuring the WebSEAL Logout page.”

Configuring the WebSEAL Logout page

Whenever a user successfully logs on to WebSEAL, and in turn through Single Sign-on (SSO) to PeopleSoft, a session cookie from PeopleSoft is stored in the browser’s memory. Unless the user physically closes the browser, the session between the browser and PeopleSoft remains open, even if the user has logged out of Tivoli Access Manager. If another user were to re-use the same browser window to log on to WebSEAL and access PeopleSoft, PeopleSoft might assume that the new user was the same as the previous user.

To solve this problem, the integration package includes a `logout.html` file, similar to the `logout.html` file that is supplied with the default WebSEAL installation. The supplied `logout.html` page includes a JavaScript that erases session cookies from the browser upon logout from WebSEAL.

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:
`WebSEAL_install_dir\www-instance\lib\html\locale\logout.html`
2. Locate the `logout.html` file in the integration package.
3. Use this `logout.html` file to overwrite the existing `logout.html` file.
4. Modify the `logout.html` file, updating the `exception_list` variable to include the list of cookies that you do not want destroyed:

```
// IBM Tivoli 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 = "";
```

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.html` file in the directory `WebSEAL_install_dir\www-instance\lib\html\locale\`.
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 server.

After configuring the WebSEAL Logout page as described above, proceed to “PeopleTools Configuration.”

PeopleTools Configuration

This section describes the integration steps required on PeopleTools. After the following changes are applied, ensure that the PeopleSoft application server and the application server (typically WebSphere®) are restarted.

Create a New User Profile

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

To create the new user profile:

1. Log in to PeopleSoft using a browser. From the menu, select **PeopleTools** then **Security** then **User Profiles** then **User Profiles** then **Add A New Value**.
2. Enter a User ID that will be used for public access to the PeopleSoft application. For example, `sso_default_user`.
3. 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.
4. Select the **ID** tab. Select an **ID Type** of *None*.
5. 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.
6. Save the new user by clicking **Save**.

Update the PeopleTools Configuration

PeopleTools must be configured by editing the appropriate Web Profile as follows:

1. Log into PeopleSoft using a browser.
2. From the menu, select **PeopleTools**, then **Web Profile**, then **Web Profile Configuration**.
3. Click the **Search** button.
4. Click the appropriate Web Profile (for example, DEV).
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 Users**. 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. 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 of the **Look and Feel** tab, enter the name of the new logout page in the **Logout Page** field (for example, `logout_redirect.html`).
 - b. Copy the `logout_redirect.html` page from the integration package to the directory:

`Peoplesoft_app_deployed_dir\PORTAL\WEB-INF\psftdocs\ps`

The new file contains sample code to redirect the user to the WebSEAL or Web Plug-ins logout page. Ensure the user is redirected to the correct path by setting the HREF as follows:

```
<A HREF="../../../../pkmslogout">
```

For example:

```
<HTML>
<HEAD><TITLE>Logout Page</TITLE></HEAD>
<BODY>
<H1>Logout Page</H1>
User is logged out, but still needs to log out from
WebSEAL/Web Plug-in to be completely logged out.
You may want to redirect the user to the
<A HREF="../../../../pkmslogout">
WebSEAL Logout Page
</A>
at this point.
</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 header being passed by WebSEAL. To do this:

1. In the Application Designer, open a definition of type *Record* and name `FUNCLIB_LDAP`.
2. Choose **View** then **PeopleCode Display**.
3. In the displayed grid, double-click the checkbox at the junction of the **LDAPAUTH** row and the **FDe** column. This displays the PeopleCode functions.
4. At the end of the file, add a function that reads the `iv-user` header passed by WebSEAL and logs all activity for troubleshooting purposes. Do not remove trace information until SSO is working correctly. The integration package includes a sample file, `tivoliSS0.peoplecode`, that can be used to copy-and-paste the required code.
5. Locate the function called `getWWWAAuthConfig()`. Set the default user ID to the name of the new user profile that you created earlier. For example:


```
Function getWWWAAuthConfig()
  &defaultUserId = "sso_default_user";
End-Function;
```
6. Click **Save** to write the changes to the database.
7. Close the Application Designer.

Enable SignOn to PeopleCode

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

1. Login to PeopleSoft using a browser. From the menu, select **PeopleTools** then **Security** then **Security Objects** then **Signon PeopleCode**.
2. Add a new row by clicking on the plus sign on the last row.
3. 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*, or whatever else you called the new function when it was added in the previous section.
 - 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 *configuration.properties*).
4. Select the **Invoke As** radio button and enter the user name for the PeopleSoft administrator (for example, user PS for HRMS, or VP1 for Financials) and the corresponding password.
5. Click the **Save** button.

Remove PeopleSoft Inactivity Timeout

PeopleTools inactivity timeout functionality can be disabled when accessing the PeopleSoft applications via WebSEAL or the Web Plug-in. This is because WebSEAL or the Web Plug-in will handle the user inactivity with its own session management functionality.

Additionally, PeopleTools generates a cookie to store the host name of the accessed PeopleSoft application server. JavaScript checks that the current server host value matches the server host that is stored in the cookie. When this integration is applied using WebSEAL, the user no longer accesses PeopleSoft applications directly, but is granted access through the WebSEAL server. Therefore, this causes the JavaScript code to fail and redirects the user to the **Session Expiration** page.

The PeopleSoft application server must be made aware of WebSEAL (or the Web Plug-in) in order to disable PeopleSoft inactivity and ensure the immediate session expiration redirection does not occur.

Perform the following steps:

1. Open the Application Designer.
2. Choose **File** then **Open**.
3. Select a definition of type **HTML**.
4. Enter the definition of **PT_SAVEWARNINGSCRIPT**. 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.
5. Add the following code to the end of the file:


```

//% IBM Tivoli Access Manager Integration
//% Check for WebSEAL junction cookie presence

function isViaWebSEAL()
{
    var allcookies;
    allcookies = document.cookie;

    if ((allcookies == null) || (allcookies == ""))
        return false;

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

```

CAUTION:

Do not copy-and-paste the text above. The integration package includes a `isViaWebSEAL.js` file that can be used for this purpose.

- Find the function `setTimeout()`. Add the following code to the beginning of the function:

```

if (isViaWebSEAL())
    return;

```

- Choose **File** then **Save**.
- Choose **File** then **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:

- Open the Application Designer.
- Choose **Go** then **Definition Security**. A new window is displayed.
- Choose **File** then **Open** then **Permission Lists**.
- Select ALLPAGES for FDM, or HCPPALL for HR.
- 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.
- Choose **File** then **Save**.
- Choose **File** then **Exit**.

Restart Application Servers

Restart the Application Servers as follows:

- Remove all files within the Web application server cache. For example:
C:\PT8.47\webserv\server\peoplesoft.ear\PORTAL\ps\cache
- Stop the PeopleSoft domain by using the `psadmin` utility.
- Remove all directories in the `PeopleSoft_home\appserv\Domain_Name\CACHE` directory.
- Restart the PeopleSoft domain.
- Restart the Web application server.

Checking the Integration

To confirm that your Tivoli Access Manager integration with PeopleSoft has been successfully configured:

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

Web Plug-in

`http[s]://peoplesoft_host_fqdn/ps/ps/?cmd=start`

For example:

`http[s]://www.example.com/ps/ps/?cmd=start`

WebSEAL with Standard Junction

`http[s]://webseal_host_fqdn/junction_name/ps/ps/?cmd=start`

WebSEAL with Transparent Path Junction

`http[s]://webseal_host_fqdn/ps/ps/?cmd=start`

WebSEAL with Virtual Host Junction

`http[s]://peoplesoft_fqdn/ps/ps/?cmd=start`

2. An authentication comes from WebSEAL or the Web Plug-in. Log in using your Tivoli Access Manager user ID and password.
3. Upon successful authentication, the PeopleSoft application main page should be displayed.

Uninstallation

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 or the Web Plug-in, you may also wish to restore your original WebSEAL or Web Plug-in settings.

Chapter 3. Troubleshooting

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

- In environments where the new PeopleCode function `TivoliSSO()` will run on UNIX systems, ensure that the filename for the log file in the sample PeopleCode conforms to the operating system standards. Leaving it as `C:\TEMP\...` on a UNIX system will result in failure to achieve single sign-on.
- 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:
 1. Forgetting to set the **defaultUserId** value in the `getWWWAAuthConfig()` PeopleCode function,
 2. Forgetting to enable the PeopleCode.

Note: 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 getWWWAAuthConfig().
sso_default_user
INFO: %SignonUserId = &defaultUserId
INFO: userID is valid.
PS
INFO: TivoliSSO() exit.
INFO: TivoliSSO() entry.
INFO: PSAuthResult and authMethod OK.
INFO: after getWWWAAuthConfig().
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 getWWWAAuthConfig().
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 getWWWAAuthConfig().
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.
```

- When creating a new user profile on the PeopleSoft database (as described in “Create a New User Profile” on page 13), 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.
- If the server returns an error such as *500 internal server error* when logging off PeopleSoft, check that the `logout.html` text was entered twice (that is `logout.html, logout.html`) in the **Logout Page** field, as described in the PeopleSoft Configuration sections of this document.
- If the login page is displayed after signing in to Tivoli 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 PeopleSoft default `signoff.html` page.

Appendix A. Support information

This section describes the following options for obtaining support for IBM products:

- “Searching knowledge bases”
- “Obtaining fixes”
- “Contacting IBM Software Support” on page 22

Searching knowledge bases

If you have a problem with your IBM software, you want it resolved quickly. Begin by searching the available knowledge bases to determine whether the resolution to your problem is already documented.

Search the information center on your local system or network

IBM provides extensive documentation that can be installed on your local computer or on an intranet server. You can use the search function of this information center to query conceptual information, instructions for completing tasks, reference information, and support documents.

Search the Internet

If you cannot find an answer to your question in the information center, search the Internet for the latest, most complete information that might help you resolve your problem. To search multiple Internet resources for your product, expand the product folder in the navigation frame to the left and select **Web search**. From this topic, you can search a variety of resources including:

- IBM technotes
- IBM downloads
- IBM Redbooks®
- IBM developerWorks®
- Forums and newsgroups
- Google

Obtaining fixes

A product fix might be available to resolve your problem. You can determine what fixes are available for your IBM software product by checking the product support Web site:

1. Go to the IBM Software Support Web site (<http://www.ibm.com/software/support>).
2. Under **Products A - Z**, select your product name. This opens a product-specific support site.
3. Under **Self help**, follow the link to **All Updates**, where you will find a list of fixes, fix packs, and other service updates for your product. For tips on refining your search, click **Search tips**.
4. Click the name of a fix to read the description and optionally download the fix.

To receive weekly e-mail notifications about fixes and other news about IBM products, follow these steps:

1. From the support page for any IBM product, click **My support** in the upper-right corner of the page.
2. If you have already registered, skip to the next step. If you have not registered, click register in the upper-right corner of the support page to establish your user ID and password.
3. Sign in to **My support**.
4. On the My support page, click **Edit profiles** in the left navigation pane, and scroll to **Select Mail Preferences**. Select a product family and check the appropriate boxes for the type of information you want.
5. Click **Submit**.
6. For e-mail notification for other products, repeat Steps 4 and 5.

For more information about types of fixes, see the *Software Support Handbook* (<http://techsupport.services.ibm.com/guides/handbook.html>).

Contacting IBM Software Support

IBM Software Support provides assistance with product defects.

Before contacting IBM Software Support, your company must have an active IBM software maintenance contract, and you must be authorized to submit problems to IBM. The type of software maintenance contract that you need depends on the type of product you have:

- For IBM distributed software products (including, but not limited to, Tivoli, Lotus®, and Rational® products, as well as DB2® and WebSphere products that run on Windows® or UNIX operating systems), enroll in Passport Advantage® in one of the following ways:
 - **Online:** Go to the Passport Advantage Web page (http://www.lotus.com/services/passport.nsf/WebDocs/Passport_Advantage_Home) and click **How to Enroll**
 - **By phone:** For the phone number to call in your country, go to the IBM Software Support Web site (<http://techsupport.services.ibm.com/guides/contacts.html>) and click the name of your geographic region.
- For IBM eServer™ software products (including, but not limited to, DB2 and WebSphere products that run in zSeries®, pSeries®, and iSeries® environments), you can purchase a software maintenance agreement by working directly with an IBM sales representative or an IBM Business Partner. For more information about support for eServer software products, go to the IBM Technical Support Advantage Web page (<http://www.ibm.com/servers/eserver/techsupport.html>).

If you are not sure what type of software maintenance contract you need, call 1-800-IBMSERV (1-800-426-7378) in the United States or, from other countries, go to the contacts page of the IBM Software Support Handbook on the Web (<http://techsupport.services.ibm.com/guides/contacts.html>) and click the name of your geographic region for phone numbers of people who provide support for your location.

Follow the steps in this topic to contact IBM Software Support:

1. Determine the business impact of your problem.
2. Describe your problem and gather background information.
3. Submit your problem to IBM Software Support.

Determine the business impact of your problem

When you report a problem to IBM, you are asked to supply a severity level. Therefore, you need to understand and assess the business impact of the problem you are reporting. Use the following criteria:

Severity 1	Critical business impact: You are unable to use the program, resulting in a critical impact on operations. This condition requires an immediate solution.
Severity 2	Significant business impact: The program is usable but is severely limited.
Severity 3	Some business impact: The program is usable with less significant features (not critical to operations) unavailable.
Severity 4	Minimal business impact: The problem causes little impact on operations, or a reasonable circumvention to the problem has been implemented.

Describe your problem and gather background information

When explaining a problem to IBM, be as specific as possible. Include all relevant background information so that IBM Software Support specialists can help you solve the problem efficiently. To save time, know the answers to these questions:

- What software versions were you running when the problem occurred?
- Do you have logs, traces, and messages that are related to the problem symptoms? IBM Software Support is likely to ask for this information.
- Can the problem be re-created? If so, what steps led to the failure?
- Have any changes been made to the system? (For example, hardware, operating system, networking software, and so on.)
- Are you currently using a workaround for this problem? If so, please be prepared to explain it when you report the problem.

Submit your problem to IBM Software Support

You can submit your problem in one of two ways:

- **Online:** Go to the "Submit and track problems" page on the IBM Software Support site (<http://www.ibm.com/software/support/probsub.html>). Enter your information into the appropriate problem submission tool.
- **By phone:** For the phone number to call in your country, go to the contacts page of the IBM Software Support Handbook on the Web (techsupport.services.ibm.com/guides/contacts.html) and click the name of your geographic region.

If the problem you submit is for a software defect or for missing or inaccurate documentation, IBM Software Support creates an Authorized Program Analysis Report (APAR). The APAR describes the problem in detail. Whenever possible, IBM Software Support provides a workaround for you to implement until the APAR is resolved and a fix is delivered. IBM publishes resolved APARs on the IBM product support Web pages daily, so that other users who experience the same problem can benefit from the same resolutions.

For more information about problem resolution, see Searching knowledge bases and Obtaining fixes.

Appendix B. 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 (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
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 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 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.

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.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

The following terms are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both:

AIX
DB2
IBM

IBM(logo)
SecureWay
Tivoli
Tivoli (logo)
Universal Database
WebSphere

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

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries.

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

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



Printed in USA