

for Version 5.1



**SAP NetWeaver Application Server Java
(including SAP NetWeaver Portal)
Integration Guide**

for Version 5.1



**SAP NetWeaver Application Server Java
(including SAP NetWeaver Portal)
Integration Guide**

Note

Before using this information and the product it supports, read the information in Appendix D, “Notices,” on page 27

This edition applies to version 3.0.05 of the Tivoli Access Manager Integration with SAP NetWeaver Application Server Java and to all subsequent releases and modifications until otherwise indicated in new editions.

© **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 book | v |
| Publications | v |
| Base Information | v |
| WebSEAL Information | v |
| Accessing Publications Online | vi |
| Contacting Software Support. | vi |
| Tivoli technical training | vi |
| Conventions Used in this Book. | vii |

Chapter 1. Introducing Tivoli Access Manager Integration with SAP NetWeaver

| | |
|---|----------|
| Application Server Java | 1 |
| Introduction | 1 |
| Integration Product Version Information | 3 |
| Integration Package Contents | 3 |
| Integration Process Flow | 3 |
| Integration Checklist. | 5 |

Chapter 2. Integration Process **7**

| | |
|---|----|
| Before You Start | 7 |
| Tivoli Access Manager WebSEAL Configuration | 8 |
| Creating a WebSEAL Junction | 8 |
| Configuring WebSEAL Options. | 11 |
| Configuring the logout page. | 11 |
| SAP NetWeaver Application Server Java Configuration | 12 |
| Adjusting the Login Module Stack to use Header Variables | 12 |
| Adjusting the JSessionId cookie from domain to host only cookie | 14 |
| Altering the password change functionality. | 14 |
| Customizing the SAP NetWeaver Application Server Java logout | 15 |
| Restarting the SAP NetWeaver Application Server Java cluster | 15 |
| Checking the integration | 15 |
| Removing the Integration. | 16 |
| Known Issues | 16 |

Appendix A. Configuring WebSEAL for integration with SAP NetWeaver Portal **19**

| | |
|--|----|
| Creating a WebSEAL Junction | 19 |
| WebSEAL Junction Mapping Table (JMT) Setup | 19 |
| WebSEAL Configuration Options | 19 |

Appendix B. Configuring the SAP UME for IBM Tivoli Directory Server **21**

Appendix C. IBM Software Support **23**

| | |
|---|----|
| Determine the business impact of your problem | 23 |
| Describe your problem and gather background information | 24 |
| Submit your problem to IBM Software Support | 24 |
| Searching knowledge bases | 24 |
| Search the information center on your local system or network | 25 |
| Search the Internet | 25 |
| Obtaining fixes | 25 |

Appendix D. Notices **27**

| | |
|----------------------|----|
| Trademarks | 29 |
|----------------------|----|

Preface

This guide tells you how to configure and manage your IBM Tivoli Access Manager installation to integrate with SAP NetWeaver Application Server Java.

This document assumes that both Tivoli Access Manager and SAP NetWeaver Application Server Java are installed, configured and running on your network. It does not provide details on the installation and administration of these products, except where necessary to achieve integration.

Who should read this book

This guide is for those responsible for the installation, deployment and administration of IBM Tivoli Access Manager, Tivoli Access Manager WebSEAL and SAP NetWeaver Application Server Java.

Readers should be familiar with the following:

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

Publications

These publications complement the information 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 Tivoli Access Manager Base Administrator's Guide*
Describes the concepts and procedures for using Access Manager services. Provides instructions for performing tasks from the Web portal manager interface and by using the **pdadmin** command.

WebSEAL Information

- *IBM Tivoli Access Manager WebSEAL Installation Guide*
Provides installation, configuration, and removal instructions for the WebSEAL server and the WebSEAL application development kit.
- *IBM Tivoli 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 Tivoli 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.

Accessing Publications Online

The publications for this product are available online in Portable Document Format (PDF) or Hypertext Markup Language (HTML) format, or both in the Tivoli Software Library: <http://www.ibm.com/software/tivoli/library>

To locate product publications in the library, click the **Product manuals** link on the left side of the Library page. Then, locate and click the name of the product on the Tivoli Software Information Center page.

Product publications include release notes, installation guides, user's guides, administrator's guides, and developer's references.

Note: To ensure proper printing of PDF publications, select the **Fit to page** check box in the Adobe Acrobat Print window (which is available when you click **File → Print**).

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 Appendix C, "IBM Software Support," on page 23.

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 SAP NetWeaver Application Server Java

This chapter has the following sections:

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

Introduction

SAP NetWeaver Application Server Java (SAP AS-Java) provides an open infrastructure for deploying J2EE Web applications. This integration guide describes the procedures for integrating IBM Tivoli Access Manager for e-business with J2EE Web applications deployed on SAP NetWeaver Application Server Java (or SAP NetWeaver Portal) to achieve Single Sign-On (SSO) capability.

A Tivoli Access Manager WebSEAL server is deployed as a reverse-proxy in front of SAP AS-Java. The WebSEAL server acts as a security gateway that authenticates and authorizes user access to the SAP AS-Java.

J2EE web applications deployed on SAP AS-Java are configured to use the SAP AS-Java User Management Engine (UME).

When a user is authenticated by WebSEAL, the authenticated user ID is passed to SAP AS-Java in an HTTP header. SAP AS-Java is configured to accept and trust this user ID from WebSEAL. The user is seamlessly signed on to the J2EE Web application that is deployed on SAP AS-Java.

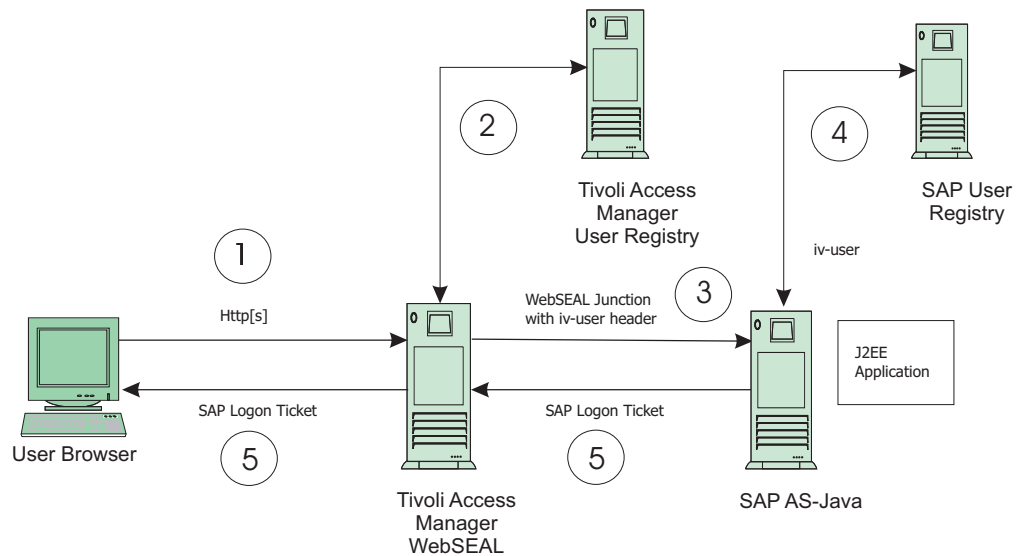


Figure 1. Architecture of the Tivoli Access Manager integration with SAP NetWeaver Application Server Java using WebSEAL.

Figure 1 above shows an integration architecture where the following processes occur:

1. A client uses their browser to access SAP AS-Java through WebSEAL.
2. WebSEAL intercepts the request, authenticates and authorizes the user.
3. On successful authentication, WebSEAL passes the request to SAP AS-Java, together with the username in the form of an HTTP header.
4. SAP AS-Java is configured to read the HTTP header and the user is authenticated to the J2EE Web application.
5. Optionally, the login module stack creates an SAP login ticket to be used by other SAP applications. The login ticket is passed back to the browser.

This guide documents the steps required to achieve this integration. To assist you in working through the process, a flowchart of required procedures and a printable checklist are also provided.

Specific procedures for SAP NetWeaver Portal are detailed on Appendix A, "Configuring WebSEAL for integration with SAP NetWeaver Portal," on page 19.

Integration Product Version Information

Integration scenarios documented in this guide are for the following product versions:

- IBM Tivoli Access Manager Base 5.1 and
- IBM Tivoli Access Manager WebSEAL 5.1
- And either:
 - SAP NetWeaver 04 SPS 16, Application Server Java
- or:
 - SAP NetWeaver 04s SPS 7, Application Server Java

Integration Package Contents

The integration package provides the following files only:

| File Name | Description |
|---|---|
| am_sapasjava_int_guide.pdf | This integration guide. |
| logout.html | A modified WebSEAL logout page. |
| azn_ent_svc_ClientProtocol.c | Sample entitlements service source code for use with protocol switching. |
| dataSourceConfiguration_tivoli_deep_not_readonly_db.xml | Sample UME configuration XML file for Tivoli Directory Server - read-write. |
| dataSourceConfiguration_tivoli_deep_readonly_db.xml | Sample UME configuration XML file for Tivoli Directory Server - read-only. |

Integration Process Flow

The diagram below illustrates the optional paths that can be followed through the various integration procedures described in this document in order to achieve integration. Each task is detailed fully in Chapter 2, “Integration Process,” on page 7.

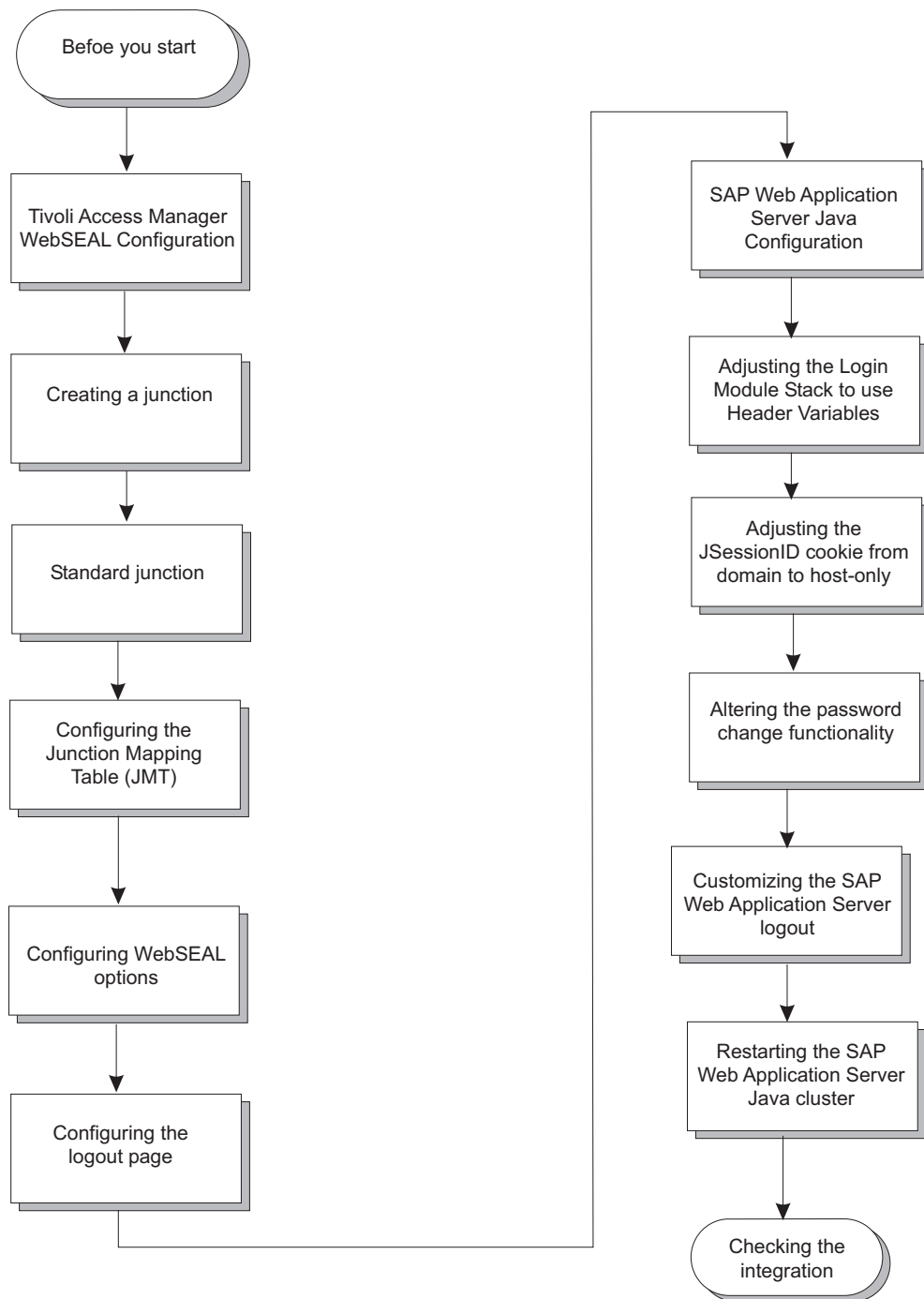


Figure 2. Pathways to integration

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 Chapter 2, “Integration Process,” on page 7.

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 WebSEAL Configuration

| Planning | Completed | Task Heading |
|--|-------------------------------|--|
| ✓ To Do | <input type="checkbox"/> Done | Creating a junction: <ul style="list-style-type: none">• Virtual host junction• Transparent path junction• Standard junction |
| <input type="checkbox"/> To Do <input type="checkbox"/> N/A | <input type="checkbox"/> Done | Configuring the Junction Mapping Table (JMT) |
| <input type="checkbox"/> To Do <input type="checkbox"/> N/A | <input type="checkbox"/> Done | Configuring WebSEAL options |
| ✓ To Do | <input type="checkbox"/> Done | Configuring the logout page |

Table 2. SAP NetWeaver Application Server Java Configuration

| Planning | Completed | Task Heading |
|----------|-------------------------------|---|
| ✓ To Do | <input type="checkbox"/> Done | Adjusting the Login Module Stack to use Header Variables |
| ✓ To Do | <input type="checkbox"/> Done | Adjusting the JSessionId cookie from domain to host only cookie |
| ✓ To Do | <input type="checkbox"/> Done | Altering the password change functionality |
| ✓ To Do | <input type="checkbox"/> Done | Customizing the SAP NetWeaver Application Server Java logout |
| ✓ To Do | <input type="checkbox"/> Done | Restarting the SAP NetWeaver Application Server Java cluster |

Chapter 2. Integration Process

This chapter has the following sections:

- “Before You Start”
- “Tivoli Access Manager WebSEAL Configuration” on page 8
- “SAP NetWeaver Application Server Java Configuration” on page 12
- “Checking the integration” on page 15
- “Removing the Integration” on page 16
- “Known Issues” on page 16

Before You Start

Before you begin this integration, review the information in Chapter 1, “Introducing Tivoli Access Manager Integration with SAP NetWeaver Application Server Java,” on page 1. Determine the procedures that you will need to follow by referring to the integration flowchart provided in “Integration Process Flow” on page 3. Then print out the tables provided in “Integration Checklist” on page 5 - 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 SAP NetWeaver Application Server Java user registry. The username in Tivoli Access Manager must match the account name for the corresponding user in the SAP user registry for mapping between the directories.
- If Tivoli Access Manager is using IBM Tivoli Directory Server (TDS), the SAP AS-Java User Management Engine (UME) can be configured to access the same user and group path used by Tivoli Access Manager by configuring it for Tivoli Directory Server. For details on how to configure the SAP UME for Tivoli Directory Server, see Appendix B, “Configuring the SAP UME for IBM Tivoli Directory Server,” on page 21.

Alternatively, the WebSEAL **Tag-Value** functionality can be used to send the SAP username, stored in an alternate user attribute, via the HTTP header. For details on HTTP **Tag-Value** functionality, refer to the *Tivoli Access Manager WebSEAL Administration Guide*.

- This guide serves as a general guide to integrate WebSEAL with applications running on SAP AS-Java. Filtering options in WebSEAL will be application-specific and must be addressed for each individual application. If filtering issues are encountered, refer to the *Tivoli Access Manager WebSEAL Administration Guide*.
- For configuration options specific to SAP NetWeaver Portal, see Appendix A, “Configuring WebSEAL for integration with SAP NetWeaver Portal,” on page 19.

The following sections detail the steps required to achieve this integration.

Tivoli Access Manager WebSEAL Configuration

This following sections describe the integration steps required on WebSEAL.

Creating a WebSEAL Junction

A WebSEAL junction must be created to connect WebSEAL with SAP AS-Java. The WebSEAL junction can be configured to use either TCP or SSL (recommended).

For this integration, the junction creation command must specify the `-c iv_user` option, which configures WebSEAL to send the authenticated username in the `iv-user` HTTP header.

Note: Before creating the junction, read “Protocol switching (optional).”

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

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

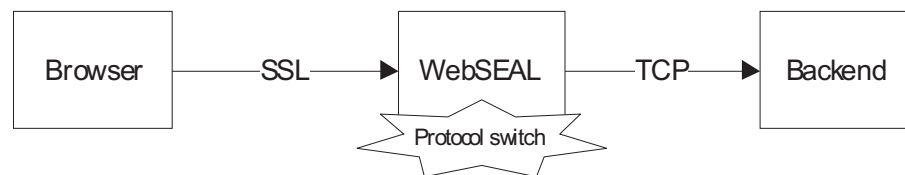
For more detailed instructions on WebSEAL junction creation, refer to the *IBM Tivoli Access Manager WebSEAL Administration Guide*.

After creating a Standard junction as described above, proceed to “Junction Mapping Table (JMT)” on page 10.

Protocol switching (optional)

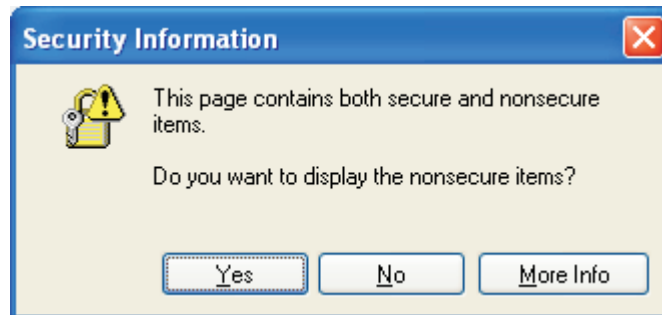
When accessing backend applications through WebSEAL, there are two distinct connections: one connection from the browser to WebSEAL; and another connection from WebSEAL to the backend application. Each connection can use a different protocol.

Protocol switching occurs when the protocol used by connection from the browser to WebSEAL is different from the protocol used by the connection from WebSEAL to the backend application. For example, protocol switching from SSL to TCP occurs when the browser is accessing WebSEAL using SSL (HTTPS) and the WebSEAL junction to SAP AS-Java is created using TCP (`-t tcp`).



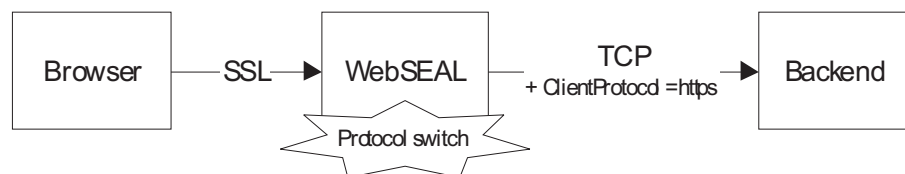
Note: Protocol switching is not available with virtual host junctions.

For the SAP AS-Java integration, when the protocol is switched by WebSEAL from SSL to TCP, a message is displayed in the browser stating that some links are not secure (see image below). This is caused by an empty value for the `src` attribute in an `iframe` tag (i.e. "`<iframe_src=...`"). Therefore, the message is incorrect and can be ignored.



However, in order to avoid the message, the protocol used by the browser to access WebSEAL must be the same as the protocol used to access the back end (that is, the protocol specified in the `-t` junction option). For example, if the browser accesses WebSEAL using HTTP over SSL (HTTPS), then an SSL junction (`-t ssl`) must be created.

An alternate approach makes use of SAP functionality that allows protocol switching by building response pages based on the value of an HTTP header called **ClientProtocol**. This is only required when the protocol is different between browser and WebSEAL and WebSEAL and Backend as described above. When the value of the header is **https**, links are generated with the https protocol, despite the method by which the request was made.



By using a TAM entitlements service and WebSEAL's HTTP-Tag-Value functionality, WebSEAL can insert the **ClientProtocol** header in the request. The details on how to create an entitlements service and configure HTTP-Tag-Value are beyond scope of this integration; however, a brief overview of the tasks required are outlined below:

1. When creating the junction, specify the option:

```
-v webseal_fqdn:ssl_port junction
```

where *webseal_fqdn* is the fully qualified domain name of the WebSEAL server, and *ssl_port* is the ssl port on which WebSEAL is listening. This enables SAP AS-Java to build pages with the correct hostname and port.

2. Install the Tivoli Access Manager Application Developer Kit (ADK) from the Tivoli Access Manager Web Security CD.
3. Create an entitlements service that inserts an attribute called **tagvalue_ClientProtocol** into the Tivoli Access Manager credential with the value *https*. A sample entitlements service source-code file is supplied with the integration package. Build the sample source-code using an appropriately modified version of the makefile (supplied with the ADK examples). The example makefile is located at:

```
tam_adk_install_dir/example/ent_svc/demo/cpp/Makefile.in
```

4. Copy the entitlements service binary to the WebSEAL bin directory (*webseal_install_dir/bin*).
5. Configure WebSEAL to use the entitlements service. For example, modify the *webseald-instance.conf* file to include the following:


```
[aznapi-configuration]
cred-attribute-entitlement-services = ClientProtocol

[aznapi-entitlement-services]
ClientProtocol = azn_ent_svc_ClientProtocol
```
6. Set the HTTP-Tag-Value junction attribute with a value of *ClientProtocol=ClientProtocol*. For example, using **pdadmin** issue the command:


```
pdadmin > object modify /WebSEAL/server-instance/junction
set attribute HTTP-Tag-Value ClientProtocol=ClientProtocol
```

For more detailed instructions on creating and configuring an entitlement service and creating the HTTP-Tag-Value junction attribute, refer to the *IBM Tivoli Access Manager WebSEAL Administration Guide* and the *IBM Tivoli Access Manager WebSEAL Developers Reference*.

Junction Mapping Table (JMT)

Server-relative URLs generated on the client-side by applets and scripts initially lack knowledge of the junction point. WebSEAL cannot filter such URLs because they are generated dynamically on the client side. During a client request for a resource using such a URL, WebSEAL can attempt to reprocess the server-relative URL using a pre-defined mapping table.

As stated in *Before You Start*, this guide does not provide any specific steps on configuring WebSEAL to correctly filter content from back end J2EE Web applications. The steps below provide an overview of the steps required to create and configure the JMT, should it be required.

Perform the following tasks to create and configure a junction mapping table:

1. Open the Tivoli Access Manager WebSEAL configuration file:


```
webseal_install_dir/etc/webseald-instance.conf
```
2. Within the [junction] stanza, set the value of the jmt-map option to *lib/jmt.conf*.
3. If there is no previously created *jmt.conf* file, create the file in the directory *webseal_install_dir/www-instance/lib*.
4. Modify the *webseal_install_dir/www-instance/lib/jmt.conf* file, creating a mapping table for the appropriate URL pattern. For example, using the SAP User Administration web application and assuming your junction name to the J2EE Web application is */jct_sapas-java*, the following lines should be created:


```
/jct_sapas_java /useradmin/*
/jct_sapas_java /logon/*
```
5. Reload the JMT. From **pdadmin**, enter the following command:


```
pdadmin> server task webseald-server_namejmt load
```

For details on configuring the Junction Mapping Table, refer to the *Tivoli Access Manager WebSEAL Administration Guide*.

After creating a JMT as described above (if required), proceed to “Configuring WebSEAL Options” on page 11.

Configuring WebSEAL Options

A WebSEAL option must be added to allow SAP Web applications to utilize SAP SSO, using an SAP login ticket. For example, SSO is required between the J2EE web application deployed on SAP AS-Java and SAP Internet Transaction Server. This option is not required if the SAP applications are not configured for SAP SSO.

Modify the `webseal_install_dir/etc/webseald-instance.conf` file by adding the following entry to the `[preserve-cookie-names]` stanza:

```
name = MYSAPSS02
```

Restart WebSEAL after making any changes to the `webseald-instance.conf` file.

Note: Further `webseald-instance.conf` configuration changes may be required in order for WebSEAL to correctly filter content from the J2EE Web applications deployed on SAP AS-Java. However, as the details of the J2EE Web application are not known, the configuration options cannot be provided by this integration guide. For details on configuring options in the `webseald-instance.conf` file, refer to the *IBM Tivoli Access Manager WebSEAL Administration Guide*.

After modifying WebSEAL configuration options (if required), proceed to “Configuring the logout page.”

Configuring the logout page

Whenever a user successfully logs on to Tivoli Access Manager WebSEAL, and in turn through Single Sign-on (SSO) to the SAP AS-Java, session cookies from the SAP AS-Java will be stored in the browser’s memory. Unless the user physically closes the browser, the session between the browser and SAP AS-Java 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 the SAP AS-Java, the SAP AS-Java 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 Tivoli Access Manager WebSEAL installation. The `logout.html` page includes a JavaScript that erases any pre-defined browser session cookies from the SAP AS-Java upon logout from WebSEAL.

Note: The Tivoli Access Manager WebSEAL returns the `logout.html` page when a user logs out using the **pkmslogout** function. This function is not available when the plug-in has been configured to use the Basic Authentication (BA). Hence this section is not relevant if WebSEAL is set to this BA mode.

To configure the Tivoli Access Manager WebSEAL logout page with the required JavaScript:

1. Make a backup copy of your existing logout page:
`webseal_install_dir/www/lib/html/locale/logout.html`
2. Locate the `logout.html` file in the integration package.
3. Overwrite the existing `logout.html` with the contents of the new `logout.html` file.

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:
`webSEAL_install_dir\www\lib\html\locale\logout.html`
2. Use an editor to open the `logout.html` file in the integration package.
3. Copy the script element from the HTML code (contained between the script start and end tags):

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

4. Paste this code into your existing `logout.html` file.
5. In the body tag, add the parameter
`onLoad="delete_all_cookies('/', exception_list)"`

For example:

```
<BODY bgColor="#FFFFFF" text="#000000"
onLoad="delete_all_cookies('/', exception_list)">
```

6. Save the new `logout.html` file.

After configuring the WebSEAL logout page as described above, proceed to “SAP NetWeaver Application Server Java Configuration.”

SAP NetWeaver Application Server Java Configuration

This section details the integration steps required on SAP NetWeaver Application Server Java.

Adjusting the Login Module Stack to use Header Variables

When a user is authenticated on SAP AS-Java, the server processes the stack of login modules that apply to the J2EE web application that the user accesses. The header variable login module is not automatically included with the default login module stacks. Therefore, to use header variables for authentication, you must adjust the login module stacks for those applications that will use header variables to authenticate a user.

1. Create the **HeaderVariableLoginModule** in the active user store:
 - a. In the Visual Administrator, select **Server (name) - Services - Security Provider**.
 - b. Select the **User Management** tab.
 - c. Click the **Switch to edit mode** button.
 - d. Click **Manage Security Stores**.

The currently active user store and the login modules for that user store are displayed.

- e. Select **UME store**.
- f. Select **Add Login Module**.

A dialog box prompts you to choose an editor for the login module option.

- g. Select **OK**.

A dialog box prompts you to add a login module.

h. Fill in the fields as follows:

| Field name | Field value |
|--------------|---|
| Class Name | com.sap.security.core.server.jaas.HeaderVariableLoginModule |
| Display Name | HeaderVariableLoginModule |

i. Select **OK**.

The **HeaderVariableLoginModule** now appears in the list of login modules for the active user store.

2. Adjust the J2EE web application's login module stack by adding in the **HeaderVariableLoginModule**:

a. In the Visual Administrator, choose **Server (name) - Services - Security Provider**.

b. Select **Policy Configurations - Authentication**.

c. Select the J2EE web application that is to be configured to support header variable authentication.

Alternatively, an authentication template used by the J2EE Web application may be selected (for example, SAP NetWeaver Portal uses the **ticket** authentication template). Modifying an authentication template will affect every application configured to use the template.

d. Add the login module **HeaderVariableLoginModule** to the login module stack by clicking on **Add New** and selecting **HeaderVariableLoginModule**.

e. Set the options for the **HeaderVariableLoginModule** as follows:

| Option | Value |
|--------------------------|---------|
| Header | iv-user |
| ume.configuration.active | true |

f. Set the **Flag** value to be *REQUIRED*.

g. Remove all other login modules or modify the **HeaderVariableLoginModule** to ensure it is in the correct position according to the desired login behavior.

For more details on LoginModules and login behavior, refer to the online documentation at the SAP Web site.

Note: If the J2EE web application is required to participate in SAP SSO using login tickets, ensure the SAP login ticket is added to the login module stack by adding the **EvaluateTicketLoginModule** and **CreateTicketLoginModule**, and modifying the **LoginModule**'s positions as outlined below. Additionally, ensure the **MYSAPSSO2** cookie is preserved by WebSEAL as outlined in "Configuring WebSEAL Options" on page 11.

| Login Modules | Position | Flag | Options |
|---------------------------|----------|------------|---|
| EvaluateTicketLoginModule | 1 | SUFFICIENT | {ume.configuration.active=true} |
| HeaderVariableLoginModule | 2 | REQUIRED | {ume.configuration.active=true, Header=iv-user} |
| CreateTicketLoginModule | 3 | SUFFICIENT | {ume.configuration.active=true} |

After adjusting the login module stack to use header variables as described above, proceed to “Adjusting the JSessionId cookie from domain to host only cookie.”

Adjusting the JSessionId cookie from domain to host only cookie

Where there are more than one Java servers using JSESSIONID and also using WebSEAL as a reverse proxy, the generation of the JSESSIONID cookie must be adjusted so that it is not a domain cookie. This is achieved by amending the settings in the web-j2ee-engine.xml file as described below.

Note: This problem would manifest itself in the Java server of the application being unable to interpret the JSESSIONID that is being passed or used.

Adjust the cookie as follows:

1. Start the Config Tool. For example, in Windows:
`SAPJ2EEEngine_installation\j2ee\configtool\configtool.bat`
2. Switch to configuration editor mode (click the **Configuration Editor** icon).
3. Navigate to **cluster_data**, then **server**, then **persistent**, then **servlet_jsp**, then **web-j2ee-engine.xml**.
4. Switch to edit mode (click the icon to switch between view and edit mode).
5. Above the last tag `</web-j2ee-engine>` insert the following:

```
<cookie-config>
<cookie>
  <type>APPLICATION</type>
  <domain>NONE</domain>
  <path>APPLICATION</path>
</cookie>
<cookie>
  <type>SESSION</type>
  <domain>NONE</domain>
  <path>APPLICATION</path>
</cookie>
</cookie-config>
```

6. Switch back to **config tool mode** (click the **Configuration Editor** icon again).

After adjusting the JSessionId cookie from domain to host only cookie as described above, proceed to “Altering the password change functionality.”

Altering the password change functionality

By default, an SAP UME security policy forces users to change their SAP password when the password has been created by an SAP administrator, including passwords created for new SAP users. As a result, when authenticating via SSO, the user is forced to authenticate to SAP AS-Java, after successful authentication to WebSEAL, in order to change the password set by the SAP Administrator. This may not be a desirable behavior particularly in situations where all access to SAP AS-Java applications is via SSO. Therefore, configure the SAP UME to not require password changes.

Perform the following steps to achieve this:

1. Start the Config Tool. For example, in Windows:
`SAPJ2EEEngine_installation\j2ee\configtool\configtool.bat`
2. Navigate to **cluster-data** then **Global server configuration** then **services** then **com.sap.security.core.ume.service**.

3. Locate the key `ume.logon.security_policy.password_change_required` and set the value to *FALSE*.
4. Apply the change by selecting **File** then **Apply**.
5. Click **Ok**.
6. Click **Ok** again.

After altering the password change functionality as described above, proceed to “Customizing the SAP NetWeaver Application Server Java logout.”

Customizing the SAP NetWeaver Application Server Java logout

The default SAP UME logout function must be customized to achieve Single Sign-Off (SSOff) from both SAP AS-Java and Tivoli Access Manager WebSEAL.

Perform the following steps to achieve this:

1. Start the Config Tool. For example, in Windows:
`SAPJ2EEEngine_installation\j2ee\configtool\configtool.bat`
2. Navigate to **cluster-data** then **Global server configuration** then **services** then **com.sap.security.core.ume.service**.
3. Locate the key `ume.logoff.redirect.url` and set the value to either:
 - `/pkmslogout` (if using a transparent path or virtual host junction) or
 - `../pkmslogout` (if using a standard junction).
4. Apply the change by selecting **File** then **Apply**.
5. Click **Ok**.
6. Click **Ok** again.

After customizing the SAP NetWeaver Application Server Java logout as described above, proceed to “Restarting the SAP NetWeaver Application Server Java cluster.”

Restarting the SAP NetWeaver Application Server Java cluster

Restart the SAP AS-Java cluster for the changes made with the Config Tool to take affect.

After restarting the SAP NetWeaver Application Server Java cluster, proceed to “Checking the integration.”

Checking the integration

To test the integration:

1. Ensure there is no direct access to the SAP AS-Java machine. This can be done by adding an entry in the local hosts file, redirecting any references to the SAP AS-Java machine to WebSEAL.
2. Open a browser and access the SAP NetWeaver Application Server Java through WebSEAL:

Standard junction:

`http[s]://webseal_fqdn/junction/application`

For example (using the useradmin example):

`http://webseal.example.com/jct_sapas_java/useradmin`

Transparent path junction:

`http[s]://webseal_fqdn/application`

For example (using the SAP useradmin example):

`http://webseal.example.com/useradmin`

Virtual host junction:

`http[s]://sapas-java_fqdn:port/application`

For example (using the SAP useradmin example):

`http://sapas-java.example.com:50000/useradmin`

3. An authentication request is received from the Tivoli Access Manager WebSEAL. Log in using the Tivoli Access Manager user ID and password.
4. Upon successful authentication, the J2EE Web application main page should be displayed.

The integration is now complete.

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 SAP NetWeaver Application Server Java settings. If you plan to modify your network settings and redeploy WebSEAL, you may also wish to restore your original WebSEAL settings.

Known Issues

This section describes any known issues with the integration.

SYMPTOM:

When creating an SSL junction in WebSEAL, the following message is returned:

DPWWA1222E A third-party server is not responding.

Possible causes: the server is down, there is a hung application on the server, or network problems. This is not a problem with the WebSEAL server.

DPWIV1217W SSL connection error.

Also, the WebSEAL log file contains the following warning:

DPWIV1210W Function call, gsk_secure_soc_init, failed error:

000001a4 GSK_ERROR_SOCKET_CLOSED.

This symptom was identified on SAP NetWeaver Application Server Java version 6.40 SPS11.

PROBLEM:

The SAP AS-Java server fails when using the `SSL_RSA_WITH_AES_256_CBC_SHA` cipher suite. This suite is the preferred cipher suite for WebSEAL.

RESOLUTION:

Disable the `SSL_RSA_WITH_AES_256_CBC_SHA` cipher suite in SAP AS-Java. To disable the suite:

1. In the SAP Visual Administrator, select **Server (name) - Services - SSL Provider**.
2. In the **Runtime** tab, select **Dispatcher (name)**.

3. Select the **Cipher Suite** tab.
4. Locate the **SSL_RSA_WITH_AES_256_CBC_SHA** suite and select **Remove**.

Alternatively, the SAP J2EE Engine can be configured to use the unlimited strength jurisdiction policy files. For more information on configuring SSL in the SAP J2EE Engine with the unlimited strength jurisdiction policy files, refer to online SAP documentation at:

http://help.sap.com/saphelp_nw04/helpdata/en/8d/cb71b8046e6e469bf3dd283104e65b/content.htm

Appendix A. Configuring WebSEAL for integration with SAP NetWeaver Portal

The following section outlines the additional configuration steps required for integration with SAP NetWeaver Portal.

Creating a WebSEAL Junction

When creating a standard or transparent path junction, additionally specify the `-j` option.

Example command (entered as one line):

```
pdadmin> server task webseald-server_name create -t tcp -h  
sapep6_hostname -p port_no -c iv_user -j /junction_name
```

There are no further requirements when creating a virtual host junction for SAP NetWeaver Portal.

WebSEAL Junction Mapping Table (JMT) Setup

When using a standard junction, a JMT entry is required. Specify the following URL pattern:

```
/irj/*
```

For example, assuming your junction name to the SAP NetWeaver Portal is `/sapportal`, the following line should be created:

```
/sapportal /irj/*
```

WebSEAL Configuration Options

To allow WebSEAL to correctly filter the content from SAP NetWeaver Portal, several WebSEAL options have to be added and updated.

Modify the `webseal_install_dir/etc/webseald-instance.conf` file as follows:

1. Within the `[filter-content-types]` stanza, add the following option to the existing list:
`type = text/xml`
2. Within the `[filter-request-headers]` stanza, add the following option:
`header = accept-encoding`
3. Within the `[script-filtering]` stanza, set the option `script-filter` to the value `yes`. For example:
`script-filter = yes`
4. Within the `[session]` stanza, set the option `ssl-id-sessions` to the value `no`. For example:
`ssl-id-sessions = no`
5. Within the `[filter-url]` stanza, add the following vales in the appropriate alphabetic location:

```
TREENODE = IMAGEURL  
TREENODE = FOLDERCLOSEIMAGEURL  
TREENODE = FOLDEROPENIMAGEURL  
TREEUPDATE = FOLDERCLOSEIMAGEURL  
TREEUPDATE = FOLDEROPENIMAGEURL
```

6. Within the [server] stanza, set the option `process-root-requests` to the value *never*. For example:
`process-root-requests = never`
7. Save the file.
8. Restart WebSEAL.

Appendix B. Configuring the SAP UME for IBM Tivoli Directory Server

The SAP User Management Engine (UME) can be configured to use an LDAP server as a data source; however, there is no option to set-up the UME to use an LDAP directory as data source during installation. Instead you have to install with a database and configure the UME manually after installation. This section provides information on how to set-up the UME to use an IBM Tivoli Directory Server as the LDAP directory data source.

Note: SSL communication is recommended between the UME and Tivoli Directory Server. To import the Root Certificate of Tivoli Directory Server, follow the procedure outlined in the SAP documentation. This is currently located at:
http://help.sap.com/saphelp_nw04/helpdata/en/7d/77fa735e5f47a2a50b5336fd1b5a61/content.htm.

Perform the following steps to configure the UME for Tivoli Directory Server:

1. Create a UME configuration XML file containing the appropriate values for Tivoli Directory Server. An overview of the appropriate values for TDS is described at:

<https://www.sdn.sap.com/irj/sdn/weblogs?blog=/pub/wlg/2144>

Note that the specific values used in the configuration file may differ depending on your environment; for example, when using user-based data partitioning. Therefore, in order to quicken the process, a sample UME configuration XML file has been supplied with the integration package that assume Tivoli Directory Server will be used to store user and group information with the remaining information stored in the default database.

- a. Start the Config Tool (if it is not already started). For example, in Windows:
`SAPJ2EEEngine_installation\j2ee\configtool\configtool.bat`
 - b. Switch to **configuration editor mode** (click the **Configuration Editor** icon).
 - c. Navigate to **cluster_data**, then **server**, then **persistent**, then **com.sap.security.core.ume.service**.
 - d. Switch to **edit mode** (click the icon to switch between **view** and **edit** mode).
 - e. Right-click **com.sap.security.core.ume.service** and select **Create sub-node**.
 - f. Select **File-entry**.
 - g. Enter the correct name (depending on whether read-only access is desired):
 - `dataSourceConfiguration_tivoli_deep_not_readonly_db.xml`, or
 - `dataSourceConfiguration_tivoli_deep_readonly_db.xml`.
 - h. If you are using the sample file, select the **Upload** button and locate it. Otherwise, enter the configuration text in the area provided.
 - i. Click the **Create** button.
 - j. Switch back to config mode (click the **Configuration Editor** icon).
2. Activate the UME configuration XML file as follows:
 - a. Using the Config Tool, select **UME LDAP data**.
 - b. In the **Directory Server** tab, select the new configuration file. Click **OK**.
 - c. Enter the appropriate connection details and configuration information.

- d. If using an SSL connection (recommended: see note above), ensure the **ssl** option is selected.
 - e. Click the **Test connection** button.
 - f. Click the **Test authentication** button.
 - g. Enter appropriate login credentials and click **authenticate**.
 - h. Apply the changes using **File - Apply**.
 - i. Click **Ok**.
 - j. Click **Ok** again.
3. Restart the SAP AS-Java cluster.
 4. Test the changes by authenticating to the SAP AS-Java user administration application (<http://sapwasjava:port/useradmin>) using credentials stored in Tivoli Directory Server.

If WebSEAL is configured to use the same Tivoli Directory Server user and group path as SAP AS-Java, user management should be handled with Tivoli Access Manager tools (for example, **pdadmin**), rather than using SAP AS-Java user administration. Doing so will ensure that Tivoli Access Manager users are managed correctly. To ensure that user management is handled only by Tivoli Access Manager, ensure that the read-only configuration file has been used.

The combination of Tivoli Identity Manager Agent for SAP UME and Tivoli Identity Manager Agent for Tivoli Access Manager will ensure correct management of a unified user registry. See the IBM Web site for more details on Tivoli Identity Manager Agents.

Note: There cannot be any duplication of users and groups between the SAP database and Tivoli Directory Server. This is particularly important for the default users, *Administrator* and *Guest*, and default groups, *Administrators* and *Guests*. Refer to the SAP help Web site for information on how to configure the location of the default users and groups - the appropriate page is currently located at:

http://help.sap.com/saphelp_nw04/helpdata/en/3f/83df3f3e054e1de100000000a155106/content.htm

Appendix C. 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 following Passport Advantage Web page and click **How to Enroll**:
http://www.lotus.com/services/passport.nsf/WebDocs/Passport_Advantage_Home
 - **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" on page 24
3. "Submit your problem to IBM Software Support" on page 24

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 recreated? 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 (<http://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" on page 25.

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 machine 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 **Support on the Web**. 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>).

Appendix D. 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.

COPYRIGHT LICENSE: This information contains sample application programs in source language, which illustrates 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.

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[®], Windows[®], Windows NT[®], and the Windows logo 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, or both.

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