IBM TRIRIGA Application Platform
Version 3.3

Single Sign-On Setup
User Guide
Note
Before using this information and the product it supports, read the information in “Notices” on page 20.

This edition applies to version 3, release 3, modification 0 of IBM® TRIRIGA® Application Platform and to all subsequent releases and modifications until otherwise indicated in new editions.

© Copyright International Business Machines Corporation 2011, 2012. All rights reserved.

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

ABOUT THIS GUIDE ......................................................................................................................... 1

Conventions.............................................................................................................................................. 1

Intended Audience............................................................................................................................... 1

Prerequisites........................................................................................................................................ 1

Support .............................................................................................................................................. 1

1. INTRODUCTION ............................................................................................................................. 2

2. CONFIGURING MICROSOFT IIS WITH IBM TRIRIGA (JBOSS) .................................................. 4

   Setting up IIS ........................................................................................................................................ 4

   Configuring IIS .................................................................................................................................... 4

   Troubleshooting .................................................................................................................................. 4

3. SETTING UP SSO WITH IIS ............................................................................................................ 6

   Configuring IBM TRIRIGA and IIS ..................................................................................................... 6

   Troubleshooting ................................................................................................................................ 7

4. CONFIGURING APACHE WITH IBM TRIRIGA (JBOSS) ................................................................ 9

5. SETTING UP SSO WITH APACHE .................................................................................................. 10

6. SETTING UP SSO ON WEBLOGIC USING APACHE WITH ACTIVE DIRECTORY ...................... 11

   Introduction ....................................................................................................................................... 11

7. SETTING UP WEBSPHERE SSO WITH IBM HTTP SERVER USING LDAP .................................. 15

   Introduction ....................................................................................................................................... 15

   IBM HTTP Server and WebSphere Plugin Installation ...................................................................... 15

© Copyright IBM Corporation 2011, 2012.
About This Guide

IBM® TRIRIGA® requires a user name and password to gain access to the applications. Many customers use single sign-on (SSO) to manage access by their users across the spectrum of applications in their environment.

This guide describes how to set up single sign-on (SSO) for the IBM TRIRIGA Application Platform. It includes steps to allow users to sign in to IBM TRIRIGA with an existing user name and password stored in Active Directory.

Conventions

This document uses the following conventions to ensure that it is as easy to read and understand as possible:

- **Note** - A Note provides important information that you should know in addition to the standard details. Often, notes are used to make you aware of the results of actions.

- **Tip** - A Tip adds insightful information that may help you use the system better.

- **Attention** - An Attention notice indicates the possibility of damage to a program, device, system, or data.

Intended Audience

This guide is intended for users responsible for establishing and maintaining the security of their company’s IBM TRIRIGA environment.

Prerequisites

This guide assumes the reader understands the IBM TRIRIGA Application Platform and is well versed in software security and the sign-on security of their company’s environment.

Support

IBM Software Support provides assistance with product defects, answering FAQs, and performing rediscovery. View the IBM Software Support site at [www.ibm.com/support](http://www.ibm.com/support).
1. Introduction

The information in this document guides you through configuring Web servers with Red Hat JBoss Application Server, then configuring with Single Sign-On (SSO) with those servers. SSO allows your users to sign in to IBM TRIRIGA with existing user names and passwords stored in an Active Directory or LDAP Server. As noted in this document, SSO does not always result in a seamless sign on.

Configuring IIS with SSO involves two steps:

- Configure the Web server to pass Web requests to JBoss.
- Set up SSO with the Web server.

This guide covers configuring IIS and Apache with JBoss. If you use WebSphere® or Oracle WebLogic application servers, refer to the IBM or Oracle/BEA for documentation on setting up those application servers with your Web server.

Below is a diagram of an environment with a Web server that proxies requests from end users to an application server.

![Example Environment Diagram](image-url)

The following identifies the flows in the example environment diagram above:

**Step 1** Users first enter the Web Server URL in their browsers.

**Step 2** The Web Server will challenge the browser for their sign in information. (It will either prompt the user for a username and password, or seamlessly pass it over).

**Step 3** The Web Server will verify the information with the directory server.

**Step 4** If the login was successful, the Web server will append the user credentials to the HTTP header, and allow them to the Application Server.

**Step 5** The Application Server will process the user credentials and log them into the application.
Note - Disable the ‘http’ port on the Application Server after the Web server configuration has completed.
2. Configuring Microsoft IIS with IBM TRIRIGA (JBoss)

Setting up IIS

You can find information about how to set up IIS to cooperate with Tomcat at http://tomcat.apache.org/connectors-doc/webserver_howto/iis.html.

Configuring IIS

You can find information about how to configure IIS to cooperate with Tomcat at http://tomcat.apache.org/connectors-doc/reference/iis.html.

Troubleshooting

There are many places to check when troubleshooting the Jakarta Connector. If the sign in page will not display, check the following:

Troubleshooting the Jakarta Connector

Make sure to note down the location set in the .msi installer. The default the installer uses is:

C:\Program Files\Apache Software Foundation\Jakarta Isapi Redirector\n
In this document, we change this to C:\Inetpub\Jakarta.

Make sure the worker.properties file is in the correct config folder where the Jakarta Isapi Redirector is installed.

Double check all the settings in:

C:\Inetpub\Jakarta\conf\worker.properties

The worker.properties file contains the configuration of the application server.

C:\Inetpub\Jakarta\conf\uriworkermap.properties

The uriworkermap.properties file contains the mapping from the Web root context directory to mount to the application server. We use the root / directory in this chapter.

The registry contains keys for the isapi_redirect.dll, located at:

HKEY_LOCAL_MACHINE\SOFTWARE\Apache Software Foundation\Jakarta Isapi Redirector\1.0

This key is installed by the .msi installer.

The worker_file key should point to the worker.properties file. Make sure the whole path and file name are entered correctly.
Troubleshooting the Jakarta Connector

The worker_mount_file points to the uriworkermap.properties. Make sure the whole path and file name are entered correctly.

The isapi_redirect.dll will need permissions from the Web Service Extensions. Check the status column in the All Unknown ISAPI Extensions - it should display Allowed.

Make sure the application server can be reached from the IIS server on port 8009.

To test this, click Start > Run, and enter: telnet <<APPSERVER>> <<PORT>>

where <<APPSERVER>> is the hostname or IP address of the application server and <<PORT>> is the AJP Port (the default is 8009).

The screen should go blank. If it returns an error in 10 seconds, the Web server cannot connect to the application server. Consult your network administrator if a timeout occurs.

If you configure the Jakarta virtual directory to run under a different Application Pool to its parent Web site, any requests to that directory will fail and you will see a 403 18 error in the IIS log files.
3. Setting Up SSO with IIS

Configuring IBM TRIRIGA and IIS

After configuring IIS to pass Web requests to JBoss, the next step is to set up SSO. Follow the steps below to set up SSO:

To Configure IBM TRIRIGA and IIS

**Step 1** On the application server, modify `TRIRIGAWEB.properties`. This file should be located in the `Tririga/config` folder.

**Step 2** Set the following attributes:

- `SSO=Y`
- `SSO_REMOTE_USER=Y`
- `SSO_REMOVE_DOMAIN_NAME=Y`
- `SSO_REQUEST_ATTRIBUTE_NAME=sm_user`

**Note** - If the Active Directory contains usernames with inconsistent cases (for example, if IBM TRIRIGA users have been entered in lower case, and users in Active Directory are in mixed cases), use the following setting to turn off the case sensitive check upon login:

```
USERNAME_CASE_SENSITIVE=N
```

**Step 3** After applying the above settings in `TRIRIGAWEB.properties`, restart the application server to use the new settings.

**Step 4** On the IIS server, right-click My Computer and select Manage.

**Step 5** Expand Services and Applications. Select and expand Internet Information Services (IIS) Manager.

**Step 6** Under IIS, expand Web Sites.

**Step 7** Right-click Default Web Site. Select Properties.

**Step 8** In the Default Web Site Properties panel, select the Directory Security tab. In Authentication and access control, click Edit.

**Step 9** In the Authentication Methods panel, uncheck the box next to Enable anonymous access.
To Configure IBM TRIRIGA and IIS

**Step 10** Check one of the boxes next to:

- Integrated Windows authentication
- Digest authentication for Windows domain servers
- Basic authentication (password is sent in clear text)

*Note* - If you do not know which one to set, do not choose all three. Try checking one at a time, restarting IIS after the change, and testing to see if the setting works correctly. The correct setting depends on your company’s security setup.

**Step 11** Enter the domain name in *Default Domain* and *Realm*. Which fields are available depends on the check boxes selected in Authenticated access.

**Step 12** Click OK.

**Step 13** Click OK to override the AuthFlags property for the jakarta Child Node.

**Step 14** Restart IIS and make sure JBoss has been restarted.

**Step 15** Make sure you have a login within IBM TRIRIGA that matches your domain login. For example, if your domain login is john.doe, the user name in the profile of the IBM TRIRIGA Employee record should be john.doe.

*Note* - Logins are case sensitive. Some logins in Active Directory are stored in mixed case.

**Step 16** When ready, open your browser to http://<<WEBSERVER>>/

It should take you directly to IBM TRIRIGA.

**Step 17** Some Java Applets will prompt for the Windows user name and password. This is a known security issue with the Java Plugin and IIS.

Affected applets may include: Brava! Document Viewer, Gantt, Association Viewer, and Workflow Expression Editor.

Simply enter the SSO user name and password again to gain access to these applets.

**Troubleshooting**

If you are having an issue with automatically logging in, check the following:
Troubleshooting Automatic Log In

If you see the error Invalid User name or Password, make sure the SSO settings in the TRIRIGAWEB.properties have been set and JBoss has been restarted.

The user name is case sensitive within IBM TRIRIGA. To see the actual user name passed to IBM TRIRIGA via IIS, point your browser to http://<<WEBSERVER>/html/en/default/admin/requestTest.jsp.

The user name shows in either the Request Parameters section and/or in the Header Parameters section next to getUserPrincipal.
4. Configuring Apache with IBM TRIRIGA (JBoss)

Note - This process does not work with Apache 2.0. Apache 2.2 is required. This can be downloaded from apache.org or installed through the package manager on your Linux/UNIX distribution.

To Configure Apache with IBM TRIRIGA (JBoss)

Step 1  When running the installer, choose Custom Install, and install everything (including Build Headers and Libraries).

Step 2  Create a new file called tririga.conf in the conf.d directory in the Apache install.

Step 3  The contents of tririga.conf are as follows:

```
# Load proxy modules
LoadModule proxy_module modules/mod_proxy.so
LoadModule proxy_ajp_module modules/mod_proxy_ajp.so

ProxyPass / ajp://APP SERVER:8009/
ProxyPassReverse / ajp://APP SERVER:8009/
```

Where APP SERVER is the hostname of your application server.
To Set Up SSO with Apache

Step 1  In the conf.d directory under the Apache install, create a new file named ldap.conf.

Step 2  The contents of ldap.conf are as follows:

```
# Load modules
LoadModule authnz_ldap_module modules/mod_authnz_ldap.so
LoadModule ldap_module modules/mod_ldap.so

<Location “/”>
  AuthBasicProvider ldap
  AuthType Basic
  AuthzLDAPAuthoritative off
  AuthName "TRIRIGA Active Directory Apache SSO"
  AuthLDAPURL "ldap://DOMAINCONTROLER:389/DC=yourcompany,DC=com?sAMAccountName?sub?(objectClass=*)" NONE
  AuthLDAPBindDN "apache@yourcompany.com"
  AuthLDAPBindPassword "password for apache user"
  require valid-user
</Location>
```

Step 3  Change the underlined items to suit your Active Directory setup. Create a domain user called apache, whose password never expires. The purpose of this account is to do the initial bind to the LDAP/AD domain server to do the lookup for the end user.
6. Setting Up SSO on WebLogic using Apache with Active Directory

Introduction

You can set up SSO on WebLogic using Apache front end with Active Directory to authenticate. You must first configure Apache to work with WebLogic and then configure SSO.

**Note** - These instructions use WebLogic 10.5.3 and Apache 2.2 on Solaris Intel 11. If you have trouble with the built-in version of Apache 2.2, you can try installing it from [http://sunfreeware.com/download.html](http://sunfreeware.com/download.html). Use the following instructions to install Apache 2.2 to `usr/local/Apache2/`:

```
gunzip.packageName.gz
pkgadd -d packageName -local
```

Detailed instructions for configuring Apache 2.2 to point to WebLogic are available online at [http://docs.oracle.com/cd/E13222_01/wls/docs81/plugins/apache.htm](http://docs.oracle.com/cd/E13222_01/wls/docs81/plugins/apache.htm). The following is a summary of the steps involved:

**To Configure Apache 2.2 to point to WebLogic**

**Step 1**  Copy the `mod_wl_22.so` from the plugin path (this varies for different OSes, refer to “Installing the Apache HTTP Server Plug-In” section) and paste it into the Apache modules folder (`[apacheHome]/modules`).

For Solaris Intel, the plugin path is `WL_HOME/server/lib/solaris`

**Step 2**  Open the `httpd.conf` file in `conf/` folder the and add the following lines:

```
LoadModule weblogic_module modules/mod_wl_22.so

<Location />
SetHandler weblogic-handler
</Location>

<IfModule mod_weblogic.c>
WebLogicHost localhost
WebLogicPort 7001
Debug OFF
WLLogFile /tmp/wlproxy.log
WLTempDir /tmp
</IfModule>
```

**Note** – Use port 7002 for SSL, which must be enabled on the WebLogic console.

Refer to [http://m-button.blogspot.com/2008/11/how-to-configure-weblogic-to-use-ssl.html](http://m-button.blogspot.com/2008/11/how-to-configure-weblogic-to-use-ssl.html) for configuring SSL.

**Step 3**  Restart Apache by using the following command:
To Configure Apache 2.2 to point to WebLogic

```
/usr/local/apache2/bin/apachectl -k restart
```

**Step 4** Test Apache by going to the web server URL. For example, `http://localhost/`

After you configure Apache to point to WebLogic, you must set up SSO with Apache. This is very similar to the process for setting up SSO with JBoss, which was included in Section 5. Setting up SSO with Apache.

You create a `ldap.conf` file in the `conf/` folder with the code that is included below. You change the underlined text based on your Active Directory setup. The domain user called `apache` is used to do the initial bind to the LDAP/AD domain server. Use a user whose password never expires. The following is a step-by-step explanation:

**To set up SSO on Apache**

**Step 1** In the `conf.d` directory under the Apache install, create a new file named `ldap.conf`.

**Step 2** The contents of `ldap.conf` are as follows:

```bash
######################################################
LoadModule authnz_ldap_module modules/mod_authnz_ldap.so
LoadModule ldap_module modules/mod_ldap.so

<Location />
  AuthBasicProvider ldap
  AuthType Basic
  AuthLDAPAuthoritative off
  AuthName "TRIRIGA Active Directory Apache SSO"
  AuthLDAPURL "ldap://DOMAINCONTROLER:389/DC=yourcompany,DC=com?sAMAccountName?sub?(objectClass=*)" NONE
  AuthLDAPBindDN "apache@yourcompany.com"
  AuthLDAPBindPassword "password for apache user"
  require valid-user
</Location>
#####################################################
```

**Step 3** Change the underlined items to suit your Active Directory setup. Create a domain user called `apache`, whose password never expires. The purpose of this account is to do the initial bind to the LDAP/AD domain server to do the lookup for the end user.
To set up SSO on Apache

Update the TRIRIGAWEB.properties file with the following information and save:

SSO=Y
SSO_REMOTE_USER=Y
SSO_REMOVE_DOMAIN_NAME=Y
SSO_REQUEST_ATTRIBUTE_NAME=sm_user

Step 4 Update the httpd.conf file by adding this line:

Include conf/ldap.conf

Step 5 Restart Apache and IBM TRIRIGA

After setting up SSO on Apache, you must also set it up on WebLogic. You can find additional instructions in the WebLogic Configuration & Active Directory Setup - Create a Service Principal Name (SPN) sections of http://java-hints.blogspot.com/2010/02/single-sign-on-sso-between-weblogic-and.html.

Note - These sections are necessary to set it up without certificates and trusts. Refer to the article for full instructions on setting up certificates and trust.

The following is a step-by-step summary:

To set up SSO on WebLogic

Step 1 Create a user in Active Directory with a password that never expires. Do not name it with the same name as the WebLogic admin login. Under the "Account" tab, in the "User logon name" field, enter "HTTP/urlOfServer" (for example, HTTP/10.33.21.100). Under the "Account options" list, check "Use Kerberos DES encryption types for this account". You will need to reset the password.

Step 2 Create a new Active Directory Authenticator. Under the configuration settings for the new Active Directory Authenticator at Configuration > Common, set Control Flag = SUFFICIENT

Step 3 On the Provider Specific tab at Configuration > Provider Specific, fill in the following details tailored for your environment.

Note - For the User Name Attribute, use "sAMAccountName" instead of "cn" to get the username instead of the display name.
To set up SSO on WebLogic

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>IP Address or host name. For example, 10.220.43.71</td>
</tr>
<tr>
<td>Port</td>
<td>Port number Active Directory is running on. This is usually 389 or 636 if in SSL mode.</td>
</tr>
<tr>
<td>Principal</td>
<td>For example, cn=weblogic,cn=users,dc=myhost,dc=com</td>
</tr>
<tr>
<td>Credential</td>
<td>The password for the user.</td>
</tr>
<tr>
<td>User Base DN</td>
<td>Location of users in Active Directory. For example, cn=users,dc=myhost,dc=com</td>
</tr>
<tr>
<td>User from Name Filter</td>
<td>Leave blank.</td>
</tr>
<tr>
<td>User Name Attribute</td>
<td>sAMAccountName</td>
</tr>
<tr>
<td>User Object Class</td>
<td>user</td>
</tr>
<tr>
<td>Group Base DN</td>
<td>Location of groups in Active Directory. For example, cn=groups,dc=myhost,dc=com</td>
</tr>
<tr>
<td>Group from Name Filter</td>
<td>(&amp;(cn=%g)(objectclass=group))</td>
</tr>
<tr>
<td>Static Group Name Attribute</td>
<td>cn</td>
</tr>
<tr>
<td>Static Group Name Object Class</td>
<td>group</td>
</tr>
<tr>
<td>Static Member DN Attribute</td>
<td>DN</td>
</tr>
<tr>
<td>Static Group DNs from Member DN Filter</td>
<td>(&amp;(member=%M)(objectclass=group))</td>
</tr>
</tbody>
</table>
7. Setting Up WebSphere SSO with IBM HTTP Server using LDAP

Introduction

You can set up WebSphere SSO by using WebSphere and IBM HTTP Server by using LDAP.

The software versions used for this guide are WebSphere 7 and IBM HTTP Server 7. These instructions are for AIX, but they should apply for other UNIX and Linux operating systems. This guide does not explain how to install WebSphere 7 but does include the steps in installing IBM HTTP Server, configuring it to forward requests to WebSphere, and configuring SSO.

IBM HTTP Server and WebSphere Plugin Installation

Two things are required to have IBM HTTP Server working with WebSphere: the IBM HTTP Server itself and the WebSphere Web server plugin. The WebSphere Application Server package comes included with the IBM HTTP Server (IHS) and the Web server plugin. The following notes will help with the installation:

- Install as a root user
- IHS installation instructions can be found in the installation folder (readme > InstallGuide). Note: The installers requires X Windows.
- The Web server plugin installation is part of the IBM HTTP Server installation, don’t forget to install it
- The install path is usually /opt/IBMIHS
- After you finish installing IBM HTTP Server, start the Web server admin by using the following commands:

  `<ibm_HTTP_server_path>/bin/adminctl start`

  `<ibm_HTTP_server_path>/bin/apachectl start`

Setting up IBM HTTP Server for WebSphere

Two things are required to have IBM HTTP Server working with WebSphere: the IBM HTTP Server itself and the WebSphere Web server plugin. The WebSphere Application Server package comes included with the IBM HTTP Server (IHS) and the Web server plugin. The following notes will help with the installation:

The following guide describes how to forward requests from the IBM HTTP Server to WebSphere: http://thysmichels.com/2011/02/19/setup-ibm-http-server-for-websphere-application-server-v7/

The following steps describe one example of the process.
To Set Up IBM HTTP Server for WebSphere

**Step 1** Navigate to Server > Server Types > Web Server > New and complete the form.
Use this page to create a new Web server.

**Step 2** Select a Web server template.
To Set Up IBM HTTP Server for WebSphere

Step 3 Specify a user name and password and confirm that all auto-completed fields are correct.

Step 4 Start the HTTP Server and HTTP Server Administration Services if not started. You can use the following commands:

```bash
<ibm_HTTP_server_path>/bin/adminctl start
<ibm_HTTP_server_path>/bin/apachectl start
```

Step 5 Confirm that the Web Server has started successfully, which is indicated by the green arrow image in the Status column of the Web servers page.

Step 6 Select the web server and click on Generate Plug-in.

Step 7 Select the web server and click on Propagate Plug-in.

Step 8 Test the web server. Pop up a browser tab and go to the web server URL (for example, http://localhost/ or http://10.34.1.200) and verify that it works.

Setting up SSO

Setting up SSO for WebSphere with IBM HTTP Server is similar to setting up JBOSS with Apache because IBM HTTP Server is essentially a wrapper for Apache.
You can follow the following steps to set up SSO for WebSphere with IBM HTTP Server.

### To Set Up SSO for WebSphere with IBM HTTP Server

**Step 1** On the IBM HTTP Server, in the `conf.d` directory under the Apache install, create a new file named `ldap.conf`.

**Step 2** The contents of `ldap.conf` are as follows:

```bash
######################################################
LoadModule authnz_ldap_module modules/mod_authnz_ldap.so
LoadModule ldap_module modules/mod_ldap.so

<Location "/">
  AuthBasicProvider ldap
  AuthType Basic
  AuthzLDAPAuthoritative off
  AuthName "TRIRIGA Active Directory Apache SSO"
  AuthLDAPURL "ldap://DOMAINCONTROLLER:389/DC=yourcompany,DC=com?sAMAccountName?sub?(objectClass=*)" NONE
  AuthLDAPBindDN "apache@yourcompany.com"
  AuthLDAPBindPassword "password for apache user"
  require valid-user
</Location>
######################################################
```

**Step 3** Change the underlined items to suit your Active Directory setup. Create a domain user called `apache`, whose password never expires. The purpose of this account is to do the initial bind to the LDAP/AD domain server to do the lookup for the end user.

**Step 4** Update the `TRIRIGAWEB.properties` file with the following information and save:

```
SSO=Y
SSO_REMOTE_USER=Y
SSO_REMOVE_DOMAIN_NAME=Y
SSO_REQUEST_ATTRIBUTE_NAME=sm_user
```

**Step 5** Update the `httpd.conf` file by adding this line:

```
Include conf/ldap.conf
```

**Step 6** Restart IBM HTTP Server from the WebSphere Console.

**Step 7** On the WebSphere Console, ensure that the Enable application security checkbox is not checked. Restart WebSphere if you made any changes.
8. Configuring TRIRIGA with Other SSO Systems

TRIRIGA can be used with other SSO systems that conform to one of three different mechanisms to deliver the username to the Application Server through the HTTP request header.

There are 5 properties that control the functionality of the TRIRIGA SSO integration:

- **SSO [Y|N]** - Turns the SSO integration on or off
- **SSO_REMOTE_USER [Y|N]** - If SSO is set to Y, setting this to Y will take the username from the request.getRemoteUser() call in the IBM TRIRIGA Platform
- **SSO_REMOVE_DOMAIN_NAME [Y|N]** - Set this to Y if domain names are prefixed or appended with the domain name, and the usernames within TRIRIGA only have the username. If the TRIRIGA usernames have both the Domain/username, then set this to N
- **SSO_REQUEST_ATTRIBUTE_NAME [sm_user | <<system-defined>>]** - If the username is stored in a distinct HTTP attribute variable, set SSO_REMOTE_USER to N, and set this to the name of the HTTP attribute name. For example, CA Site Minder defaults the username to sm_user. Some systems enable you to define the variable name the username is stuffed into. In this case, please set SSO_REQUEST_ATTRIBUTE_NAME to the variable name in your system.
- **SSO_USER_PRINCIPAL [Y|N]** - If the system is configured to append the UPN (User Principal Name) to the http header, set this to Y, and set SSO_REMOTE_USER to N. This will cause the IBM TRIRIGA Platform to retrieve the username from the call request.getUserPrincipal().getName()
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 grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement 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 document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

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 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.

**Trademarks**

IBM, the IBM logo, ibm.com, TRIRIGA, and WebSphere are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at “[Copyright and trademark information](https://www.ibm.com/legal/copytrade.shtml)” at www.ibm.com/legal/copytrade.shtml.

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

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

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

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