IBM TRIRIGA Application Platform
Version 3 Release 5.2

Single Sign-on User Guide

Note
Before using this information and the product it supports, read the information in "Notices" on page 17.

This edition applies to version 3, release 5, modification 2 of IBM TRIRIGA Application Platform and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Chapter 1. Authenticating users by using single sign-on

To gain access to IBM TRIRIGA applications, a user must be authenticated as a valid user of the system and must be granted permission to access applications and functions in the IBM TRIRIGA suite of applications. Many customers use single sign-on (SSO) authentication to manage access by their users to multiple applications in their environment.

Chapter 2. Types of authentication

The TRIRIGA® Application Platform uses its own native authentication by default.

With native authentication, the user enters their user name and password in an IBM TRIRIGA login screen. The TRIRIGA Application Platform authenticates the user by comparing the user name and password that the user entered with the user name and password that are stored in the IBM TRIRIGA database.

Single sign-on authentication, which is not native to IBM TRIRIGA, can also be used for authentication. With single sign-on authentication, the user logs in to applications with a user name and password that are stored in an existing Lightweight Directory Access Protocol (LDAP) directory or Active Directory. The application server or web server authenticates the user by comparing the user name and password that the user entered with the user name and password that are stored in the directory server.

Chapter 3. Requirements for and limitations of single sign-on requests in TRIRIGA Application Platform

In an SSO environment, the user name and password that the user enters must match the user name and password that are stored in the directory server. The application server or web server then authenticates the user and inserts the user name into the HTTP request header.

The user name in the HTTP request header must exactly match the user name that is stored in the IBM TRIRIGA database. When configured properly, IBM TRIRIGA reads the user name from the request header and internally authenticates it against the IBM TRIRIGA database.

IBM TRIRIGA supports the following methods of inserting the user name into an HTTP header:

- Remote User - The web server or application server authenticates the user and puts the user name in the REMOTE_USER HTTP header. The Java™ call is `request.getRemoteUser()`.
- User Principal - The web server or application server authenticates the user and puts the user name in the special UserPrincipal HTTP header. The Java call is `request.getUserPrincipal().getName()`.
- HTTP Header - The web server or application server authenticates the user and puts the user name in a specific named HTTP header attribute.

In addition to the insertion methods, IBM TRIRIGA supports several options for the user name after it is retrieved from the HTTP header:

- Removal of Domain Name - In some SSO environments, the LDAP Domain Name is provided along with the user name, however, only the *username* portion is configured in the IBM TRIRIGA database. If the full string in the HTTP header is provided in the form of *MyCompany\username*, enabling this feature strips *MyCompany* or the domain portion from *username*.
- Case Sensitivity - Some directory servers supply the user name in a mixed case, depending on a number of conditions. By default, IBM TRIRIGA user names are case-sensitive. If it is determined that the directory server is providing user names with mixed cases, you can disable the case-sensitive check in the SSO process.

Considerations:

- If you are using a web server to provide the authentication portion, disable the HTTP port on the application server after the web server configuration completes. Keeping the application server's HTTP port open might create a vulnerability point. If the HTTP port is not disabled and the user goes to that port, the user is prompted for their credentials and the user name and password are verified in the IBM TRIRIGA database.
- IBM® TRIRIGA is compatible with SSO when SSO is configured properly. After the appropriate IBM TRIRIGA properties are enabled for SSO, IBM TRIRIGA can accept tokens that are provided by properly configured application servers with SSO. IBM Support can assist with configuring IBM TRIRIGA properties for SSO. However, due to the number of supported products, technologies, and configurations that are

supported by IBM TRIRIGA, IBM Support cannot help with the configuration of SSO within your environment.

Limitations:

- IBM TRIRIGA does not support Security Assertion Markup Language (SAML) or credential-less login mechanisms such as SmartCard or Common Access Card (CAC) as a method of authentication for its non-browser clients. Non-browser clients include the following clients:
  - IBM TRIRIGA CAD Integrator/Publisher
  - IBM TRIRIGA Connector for BIM
  - IBM TRIRIGA reservation add-in for Microsoft Outlook

  SSO solutions must provide a mechanism for basic authentication for non-browser clients. SAML and SmartCard or CAC do not support basic authentication for non-browser based clients.

  The best practice if you are using SAML or SmartCard/CAC is to authenticate directly to IBM TRIRIGA on a separate process server or integration server as opposed to the SSO enabled application server. This solution requires users to use their IBM TRIRIGA user name and password to sign in.

  An alternative best practice is to set up a separate non-SAML SSO solution for non-browser client users, which can support basic or NTLM authentication. This solution requires SmartCard/CAC users to use their SmartCard/CAC user name and password to sign in.

Chapter 4. How SSO works

Many possible configurations can insert the user name into the HTTP header. Configurations on a reverse proxy web server, configurations at the application server layer, or various authentication plug-ins at each of those layers can insert the user name into the HTTP header.

In general, the process occurs in the following order.

- The user enters the web server URL in a browser or accesses the application by using a client.
- The user might be prompted to enter a user name or password or seamless sign-on might occur. Seamless sign-on, where the server does not challenge the browser or client, is not supported in some configurations.
- The web server, application server, or authentication plug-in verifies the information with the authentication source.
- If the login is successful, the web server appends the user credentials to the HTTP header and sends them to the application server.
- The application server processes the user credentials and logs in the user to the application.

Note: In the IBM TRIRIGA Workplace Reservation Manager application, if you click a link such as the Building link in the Find Room/Resource dialog, a browser instance opens in a new window and you are prompted to sign in. The sign in request occurs because of security constraints; the session and login configuration cannot be shared between Outlook and the browser.

Chapter 5. Configuring IBM TRIRIGA with an SSO solution

If you have a web server that is set up with single sign-on authentication, you can determine whether those credentials can be used to sign on to IBM TRIRIGA.

Procedure

1. Configure your web server for reverse proxy access to the application server. For configuration details, see the documentation that is provided by your application server provider.
2. After the web server and application server are communicating by using reverse proxy, enter the following URL in your web browser: `http://web_server/context_path/html/en/default/admin/requestTest.jsp`. The web page shows the HTTP headers that are passed from the web server to the application server.
3. On the application server, set the properties in the `TRIRIGAWEB.properties` file based on the SSO variables that are returned at the URL. By default, the `TRIRIGAWEB.properties` file is in the `Tririga/config` folder.

If...	Then, set the following properties.
The results show Remote User set with the login.	**SSO=**Y **SSO_REMOTE_USER=**Y Set all other SSO properties to N.
The results show UserPrincipal set with the login.	**SSO=**Y **SSO_USER_PRINCIPAL=**Y Set all other SSO properties to N.
If the results show user name on a header, make note of the header name, for example, *OTHER_SSO_USER_NAME*.	**SSO=**Y **SSO_REQUEST_ATTRIBUTE_NAME=** *OTHER_SSO_USER_NAME* Set all other SSO properties to N.

4. Restart the application server so that the changes take effect.

Chapter 6. IBM TRIRIGA single sign-on properties

Several properties control an IBM TRIRIGA SSO configuration.

The SSO properties are in the `TRIRIGAWEB.properties` file. By default, the `TRIRIGAWEB.properties` file is in the `Tririga/config` folder of the application server. The application server must be restarted before the property value changes take effect.

Property	Options	Default	Description
SSO	N, Y	N	If set to Y, the environment runs in single sign-on (SSO) mode.
SSO_BACKING_SERVER_PORT	*number*	-1	The port number that is used by the back-end server. If the SSO server port does not match the back-end server port, this property must be set. If -1 or any other negative value is set for this property, then the port number that is set for the front-end server is also set for the back-end server port.
SSO_DISABLE_UNAUTHORIZED _STATUS	N, Y	N	The `unauthorized.jsp` page sends an `HTTP Error 401` response in the HTTP Header. If set to Y, the header response is disabled. If you want the `HTTP Error 401` response sent, set this property to N.
SSO_REMOTE_USER	N, Y	Y	If set to Y, the `request.getRemoteUser()` method is used to sign in. The user name must exactly match the user name that is created in IBM TRIRIGA. When the value of **SSO_USER_PRINCIPAL** is Y, set **SSO_REMOTE_USER** to N.
SSO_REMOVE_DOMAIN_NAME	N, Y	Y	If set to Y, the prefixed or appended domain name is removed from the directory server user name that is passed by using the **SSO_REMOTE_USER** property. • If user names contain a domain name when passed from the directory server and user names in IBM TRIRIGA contain only the user name, set this property to Y. • If user names contain a domain name when passed from the directory server and user names in IBM TRIRIGA include the domain name, set this property to N.

Property	Options	Default	Description
SSO_REQUEST_ATTRIBUTE_NAME	sm_user, *variable name*	sm_user	The name of the property that is inserted into the HTTP header whose value is the IBM TRIRIGA user name. If the user name is stored in a distinct HTTP attribute variable, set **SSO_REMOTE_USER** to N, and set this property to the HTTP attribute name. In some systems, you can define the variable name in which the user name is located. In this case, set this property to the variable name in your system.
SSO_USER_PRINCIPAL	N, Y	N	If the system is configured to append the User Principal Name (UPN) to the HTTP header, set this property to Y. If set to Y, the HTTP header parameter **UserPrincipal** is used, and the user name is retrieved by calling the `request.getUserPrincipal().getName()` method. When the value is Y, set the value of the **SSO_REMOTE_USER** property to N.
USERNAME_CASE_SENSITIVE	N, Y	Y	If set to Y, sign-in user names are case-sensitive. If you want to authenticate without case sensitivity, set this property to N.

Some Java Applets prompt for the Windows user name and password, which is a known security issue with the Java plug-in and SSO. Affected applets might include: Brava! Document Viewer, Gantt, Association Viewer, and Workflow Expression Editor. Enter the SSO user name and password again to gain access to these applets.

Chapter 7. Forcing users to log in through SSO

If you want to force users to log in through SSO, you must prevent them from using the default login page. Provide an alternative login page that does not contain a user name, password, or login button.

Procedure

1. Add the following properties to the `TRIRIGAWEB.properties` file to specify the alternative login page and directory.

Property	Values	Description
ALTERNATE_INDEX_HTML	*File name*	The file name of the alternative sign-in page, for example, `index.html`.
ALTERNATE_RESOURCE_DIRECTORY	`N`, `Y`	The path to the alternative sign-in page resource directory, for example, `C:\`*`pathToTRIRIGA`*`\userfiles\alt`.

2. Restart the application server.

Chapter 8. Troubleshooting single sign-on

Several issues are known to occur with single sign-on, for example, if it is not configured properly.

Invalid user name or password error.

Make sure the SSO settings in the `TRIRIGAWEB.properties` file are set and the application server is restarted.

The user name is case-sensitive in IBM TRIRIGA. To see the actual user name that is passed from the web server to IBM TRIRIGA, open the following address in a browser: `http://web_server/html/en/default/admin/requestTest.jsp`.

You can find the user name in the **Request Parameters** section, in the **Header Parameters** section next to **`getUserPrincipal`**, or in both sections.

Map labels are shown only in English.

If Esri map labels are shown in English even though your user profile is using a different language, the **`SSO_BACKING_SERVER_PORT`** property in the `TRIRIGAWEB.properties` file might not be configured for the internal non-SSO port.

HTTP requests are no longer forwarded to IBM TRIRIGA.

After you upgrade IBM TRIRIGA on WebSphere® Application Server, IBM HTTP Server no longer forwards requests to IBM TRIRIGA.

You must reconfigure the web server in WebSphere Application Server. One method of reconfiguring the web server is to use the **WebSphere Customization Toolbox** (WCT). WCT contains the **Web Server Plug-ins Configuration Tool**, which steps through the process of deleting and re-creating the web server definition for IBM HTTP Server.

Tip: When you specify the application server location in the Configuration Scenario Selection dialog, if your configuration scenario is local then browse to the location of the `\AppServer` folder. For example, a common location for the application server is `C:\Program Files (x86)\IBM\WebSphere\AppServer`.

If you change the host name, check the `plugin-cfg.xml` file to make sure that it contains the correct host name specified. Specifically, check the **`Transport Hostname`** property. The `plugin-cfg.xml` is typically in *`pathToInstall`*`/IBM/HTTPServer/Plugins/config/webServerName/plugin-cfg.xml`.

Notices

This information was developed for products and services offered in the US. This material might be available from IBM in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

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, MD-NC119
Armonk, NY 10504-1785
US

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

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 jurisdictions 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 websites are provided for convenience only and do not in any manner serve as an endorsement of those

websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you provide 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 Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

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.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

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.

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 actual people or business enterprises is entirely coincidental.

COPYRIGHT LICENSE:

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

programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work must include a copyright notice as follows:
© (your company name) (year).
Portions of this code are derived from IBM Corp. Sample Programs.
© Copyright IBM Corp. _enter the year or years_.

Trademarks

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

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

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

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

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

Other product and service names might be trademarks of IBM or other companies.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the IBM website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

IBM Online Privacy Statement

IBM Software products, including software as a service solutions, (“Software Offerings”) may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user, or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering’s use of cookies is set forth below.

This Software Offering does not use cookies or other technologies to collect personally identifiable information.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, see IBM’s Privacy Policy at http://www.ibm.com/privacy and IBM's Online Privacy Statement at http://www.ibm.com/privacy/details in the section entitled “Cookies, Web Beacons and Other Technologies,” and the "IBM Software Products and Software-as-a-Service Privacy Statement" at http://www.ibm.com/software/info/product-privacy/.

Printed in USA