TRIRIGA Wiki Home
Facilities Management …
Facilities Maintenance
Environmental & Energ…
Real Estate Management
Capital Project Manage…
CAD Integrator-Publish…
IBM TRIRIGA Connector…
IBM TRIRIGA Anywhere
IBM TRIRIGA Applicatio…
Support Matrix
Hints and Tips
Installing
Admin Console
Builder Tools
Connector for Busine…
Connector for Esri GIS
Document Manager
Extended Formula
Gantt Scheduler
Globalization
Group Object
Label Manager
Licensing
Object Labels and Re…
Offlining
OSLC
Performance
Platform Logging
Portal and Navigation
Reporting
Reserve
Scheduler Engine (Sc…
Security
SSO
TRIRIGA on WebSph…
IIS and Maximum …
TRIRIGA on WebSph…
TRIRIGA on WebSph…
TRIRIGA on WebSph…
TRIRIGA on WebLog…
TRIRIGA on WebLog…
TRIRIGA on WebSph…
Troubleshooting SSO
Styling
System Sizing
TDI
Web Graphics
Workflow
Release Notes
Media Library
Best Practices
Upgrading
Troubleshooting
UX Framework
Index
Members
Trash
Tags
Find a Tag
analysis application
availability_section best_practices
cad change_management
changes compare

You are in: IBM TRIRIGA > IBM TRIRIGA Application Platform > SSO > Troubleshooting SSO

Troubleshooting SSO

1 | Updated 4/26/19 by Jay.Manaloto | Tags: error, ihs, issue, problem, single_sign-on, sso, tip, troubleshoot, was

Page Actions

IBM TRIRIGA Application Platform.

Troubleshooting Single Sign-On (SSO)

- **SSO Resources**
  - To Debug with requestTest.jsp.
  - requestTest.jsp: HTTP Request and Header Variables.
- **SSO Known Issues**
  - 1. Invalid user name or password error.
  - 2. Map labels are shown only in English.
  - 3. Properties or settings are not propagated.
  - 4. HTTP requests are no longer forwarded to TRIRIGA.
  - 5. Front-end server is not set exactly.
  - 6. Alternate login is being used for click-jacking prevention.
  - 7. SSL/HTTPS is causing security warnings.
  - 8. CA Single Sign-On settings are not set correctly.
  - 9. Microsoft IIS 7 is interfering with CAD Integrator error reporting.
  - 10. SAML is not supported for TRIRIGA non-browser clients.
  - 11. Target URL is being lost during authentication.

SSO Resources

The **requestTest.jsp** page is the single most important resource from the TRIRIGA Platform perspective. This page is internal to the TRIRIGA Platform that displays the different areas of the **HTTP Header**, and allows you to debug and set the third-party configuration correctly.

Point your browser to the **FRONT_END_SERVER**, the URL that the end users will use to access TRIRIGA. This should be a URL that is fronted by the web server that handles the SSO. For example:

http://frontEndServer.mycompany.com/tririga-context/html/en/default/admin/**requestTest.jsp**

To Debug with requestTest.jsp.

1. If your username shows up as a **Remote User** (see **1.** in the following screenshot), then in the **TRIRIGAWEB.properties** file, set the following values and restart the application server:

- SSO=Y
- SSO_REMOTE_USER=Y
- SSO_USER_PRINCIPAL=N

2. If your username shows up as a **Header Parameter** (as a new row around **2.**), then in the **TRIRIGAWEB.properties** file, set the following values and restart the application server:

- SSO=Y
- SSO_REQUEST_ATTRIBUTE_NAME=name_of_the_parameter_on_the_left
- SSO_REMOTE_USER=N
- SSO_USER_PRINCIPAL=N

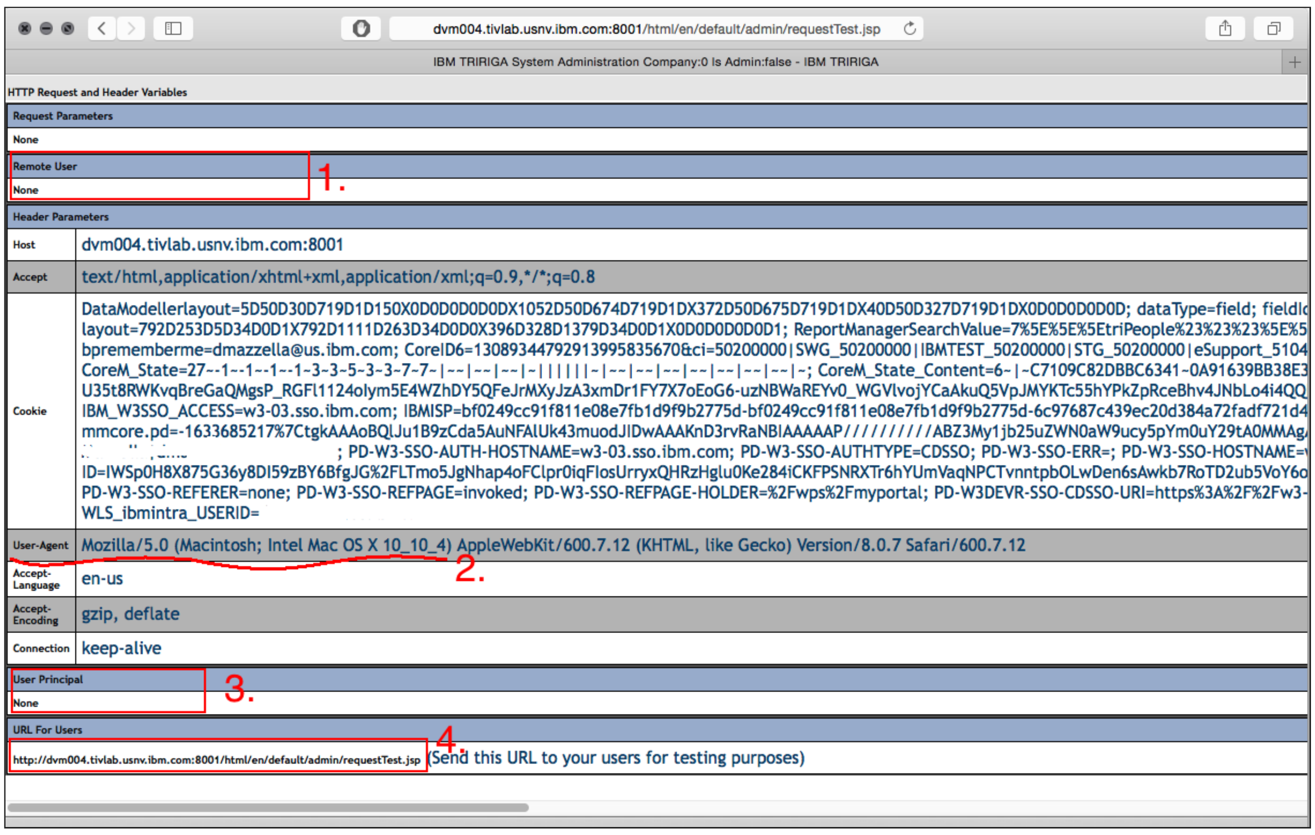
3. If your username shows up as a **User Principal** (see **3.**), then in the **TRIRIGAWEB.properties** file, set the following values and restart the application server:

- SSO=Y
- SSO_REMOTE_USER=N
- SSO_USER_PRINCIPAL=Y

4. Send the **URL For Users** (see **4.**) to other end-users for testing to make sure that you are hitting the correct server.

If you do **not** see the username on the **requestTest.jsp** page (anywhere in **1.**, **2.**, or **3.**), then the non-TRIRIGA portion of SSO is **not** correct. Start at the web server layer, and trace back by using the tools and documentation provided by the third party to make sure that the SSO is operating correctly. If the **requestTest.jsp** page cannot see the username, the SSO will **not** work.

requestTest.jsp: HTTP Request and Header Variables.



dvm004.tivlab.usnv.ibm.com:8001/html/en/default/admin/requestTest.jsp

IBM TRIRIGA System Administration Company:0 Is Admin:false - IBM TRIRIGA

HTTP Request and Header Variables

Request Parameters
None

Remote User
None

Header Parameters

Host	dvm004.tivlab.usnv.ibm.com:8001
Accept	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Cookie	DataModellerlayout=5D50D30D719D1D150X0D0D0D0D0DX1052D50D674D719D1DX372D50D675D719D1DX40D50D327D719D1DX0D0D0D0D0D; dataType=field; fieldId
	layout=792D253D5D34D0D1X792D1111D263D34D0D0X396D328D1379D34D0D1X0D0D0D0D0D1; ReportManagerSearchValue=7%5E%5E%5EtriPeople%23%23%23%5E%5
	bprememberme=dmazzella@us.ibm.com; CoreID6=13089344792913995835670&ci=50200000|SWG_50200000|IBMTEST_50200000|STG_50200000|eSupport_5104
	CoreM_State=27~-1~-1~-1~-1~3~3~5~3~3~7~7~|~~|~~|~~|~||||||~|~~|~~|~~|~~|~~|~~|~~|~; CoreM_State_Content=6~|~C7109C82DBBC6341~0A91639BB38E3
	U35t8RWKvqBreGaQMgsP_RGFl1124olym5E4WZhDY5QFeJrMXyJzA3xmDr1FY7X7oEoG6-uzNBWaREYv0_WGVlvojYCaAkuQ5VpJMYKTc55hYPkZpRceBhv4JNbLo4i4QQ
	IBM_W3SSO_ACCESS=w3-03.sso.ibm.com; IBMISP=bf0249cc91f811e08e7fb1d9f9b2775d-bf0249cc91f811e08e7fb1d9f9b2775d-6c97687c439ec20d384a72fadf721d4
	mmcore.pd=-1633685217%7CtgkAAAoBQlJu1B9zCda5AuNFAlUk43muodJIDwAAAKnD3rvRaNBIAAAAAP//////////ABZ3My1jb25uZWN0aW9ucy5pYm0uY29tA0MMAg
	; PD-W3-SSO-AUTH-HOSTNAME=w3-03.sso.ibm.com; PD-W3-SSO-AUTHTYPE=CDSSO; PD-W3-SSO-ERR=; PD-W3-SSO-HOSTNAME=
	ID=IWSp0H8X875G36y8DI59zBY6BfgJG%2FLTmo5JgNhap4oFClpr0iqFlosUrryxQHRzHglu0Ke284iCKFPSNRXTr6hYUmVaqNPCTvnntpbOLwDen6sAwkb7RoTD2ub5VoY6o
	PD-W3-SSO-REFERER=none; PD-W3-SSO-REFPAGE=invoked; PD-W3-SSO-REFPAGE-HOLDER=%2Fwps%2Fmyportal; PD-W3DEVR-SSO-CDSSO-URI=https%3A%2F%2Fw3-
	WLS_ibmintra_USERID=

User-Agent	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_4) AppleWebKit/600.7.12 (KHTML, like Gecko) Version/8.0.7 Safari/600.7.12
Accept-Language	en-us
Accept-Encoding	gzip, deflate
Connection	keep-alive

User Principal
None

URL For Users
http://dvm004.tivlab.usnv.ibm.com:8001/html/en/default/admin/requestTest.jsp (Send this URL to your users for testing purposes)

compare_revisions
customizations customize
database db2 exchange
find_available_times gantt_chart
gantt_scheduler group
memory_footprint modifications
modify object_label
object_revision
operating_system oracle
performance platform
problem_determination reports
reserve reserve_performance
revision revisioning
single_sign-on snapshot space
sql_server sso support system
system_performance
tags: track_customizations
tririga troubleshoot tuning
upgrade ux version versioning
Cloud | List

Members

SSO Known Issues

1. Invalid user name or password error.

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

The user name is case-sensitive in TRIRIGA. To see the actual user name that is passed from the web server to 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.

2. Map labels are shown only in English.

If Esri map labels are in English although 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.

3. Properties or settings are not propagated.

During a TRIRIGA upgrade, one or more SSO properties or settings in the **TRIRIGAWEB.properties** file are not propagated. After a TRIRIGA upgrade, make sure that your SSO settings are set correctly.

4. HTTP requests are no longer forwarded to TRIRIGA.

After you upgrade TRIRIGA on traditional WebSphere Application Server (tWAS) or Liberty, the HTTP Server no longer forwards requests to TRIRIGA, so it appears SSO is broken.

You must reconfigure (or regenerate) the web server plug-in.

For tWAS, the method of reconfiguring the web server plug-in 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 recreating 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 correctly specified host name. Specifically, check the **Transport Hostname** property. The **plugin-cfg.xml** file is typically found in the following location:

pathToInstall/IBM/HTTPServer/Plugins/config/***webServerName*/plugin-cfg.xml**

To generate the **plugin-cfg.xml** with a Liberty server, run the **generatePluginConfig** operation that is exposed by the **com.ibm.ws.jmx.mbeans.generatePluginConfig** MBean provided by Liberty. This JMX MBean can be invoked by using the **JConsole** utility that is supplied with the Java JDK/SDK.

Finally, for samlWeb-2.0, you will need to reinstall the feature into Liberty. Because platform upgrades give you a new version of Liberty, any old configurations or feature installs are no longer present.

5. Front-end server is not set exactly.

It is very important that the **FRONT_END_SERVER** be set exactly, character for character, to the URL that end users have in their browser. This includes the protocol (http: or https:), the fully qualified domain name (FQDN), and if used, the port number.

It should **not** include the context path. Here are some examples of when users sign into:

- http://tririga.mycompany.com, then set **FRONT_END_SERVER**=http://tririga.mycompany.com
- http://something.mycompany.com/tririga, then set **FRONT_END_SERVER**=http://something.mycompany.com
- https://secure-tririga.mycompany.com, then set **FRONT_END_SERVER**=https://secure-tririga.mycompany.com
- https://ssl.mycompany.com:8443/tririga, then set **FRONT_END_SERVER**=https://ssl.mycompany.com:8443

6. Alternate login is being used for click-jacking prevention.

Some SSO solutions use the alternate login **index.html**. You may need to add the following JavaScript code to break out of any HTML frames that are in place, to let the SSO solution operate and redirect properly:

```
<script>
if (top != self){
   top.location.href = location.href ;
   }
</script>
```

7. SSL/HTTPS is causing security warnings.

If you are receiving security warnings in parts of the application, such as the Project Tasks Gantt, make sure that you are using a valid SSL certificate. Java security may restrict self-signed certificates, so a valid purchased SSL certificate will be needed. To troubleshoot, back out the SSL configuration, make sure that a non-SSL web server is set up, and make sure that the **FRONT_END_SERVER** is configured to point to the non-SSL website.

8. CA Single Sign-On settings are not set correctly.

Make sure that the settings in CA Single Sign-On (formerly CA SiteMinder) are entered exactly as shown below. These are **not** the default values.

a. For TRIRIGA to work correctly, update these 4 settings:

- **badcsschars**='<>'.
- **badformchars**='<,>,%22'.
- **badurlchars**='./,/../*,*.,~,\,%00-%1f,%7f-%ff,%25,%25U,%25u'.
- **ignoreext**='.class,.gif,.jpg,.jpeg,.png,.fcc,.scc,.sfcc,.ccc,.ntc,.srv,.jnlp,.jar,.pdf'.

b. For both non-SSL and SSL content to work correctly, follow these steps:

- In the WebSphere console, select **Security > Global security**.
- Find the "**Authentication**" panel on the right side.
- Expand the "**Web and SIP security**" node.
- Uncheck the check box labeled "**Use available authentication data when an unprotected URI is accessed**".
- These steps apply to both WAS7 and WAS8, and are based on the **following link**.

9. Microsoft IIS 7 is interfering with CAD Integrator error reporting.

When using CAD Integrator (CI) with Microsoft IIS 7, there are instances where IIS will prevent certain expected error response codes from properly reaching the CI client. CI expects a specific format for certain error conditions. If the response comes back with a "beautified" HTML response, CI assumes that the session has been terminated.

a. To remedy this, you will have to manually edit the **web.config** file by adding this custom "**httpErrors**" entry:

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
  <system.webServer>
    <httpErrors existingResponse="PassThrough" />
  </system.webServer>
</configuration>
```

b. Next, run these commands in a command (cmd) window (assuming **inetsrv** is in the **c:\windows\system32 directory**):

```
cd C:\Windows\System32\inetsrv
appcmd unlock config /section:httpErrors
appcmd set config -section:system.webServer/httpErrors /existingResponse:"PassThrough" /commit:apphost
```

c. Finally, reset IIS.

10. SAML is not supported for TRIRIGA non-browser clients.

As stated in the TRIRIGA documentation: "**Requirements for single sign-on requests in the TRIRIGA Application Platform**":

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**, such as CAD Integrator, Connector for BIM, and the 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.

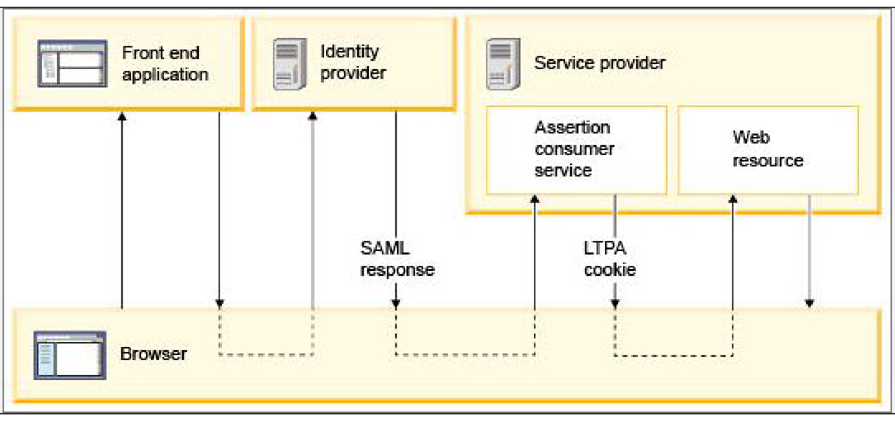
11. Target URL is being lost during authentication.

The SSO solution might be losing the target URL when it performs its authentication portion.

When the browser is sent back to the WebSphere system, there's typically a "**targetURL**" or "**RelayState**" that WebSphere picks up on and redirects. If that target is lost, WebSphere will simply redirect to the default login page. Consequently, this situation is **outside** of the realm of TRIRIGA; the target or relay state URL must be transferred in the handoff of the SSO identity provider (IdP) back to WebSphere, or in WebSphere itself.

In other words, while the front-end application is TRIRIGA, the issue might be happening somewhere with the SSO identity provider (IdP) or the service provider. Make sure that the SSO provider is properly configured to ensure the handoff is properly handing off the target URL after the SSO authentication is completed.

Identity Provider & Service Provider.



Next >

Comments (6) Versions (21) Attachments (2) About

1-6 of 6 Previous | Next

cstalker commented on March 1, 2016 Permalink
two questions, what if when I use the requestTest.jsp I get both 1 and 2 username values back, which configuration should I use? and if using configuration 2 the value for SSO_REQUEST_ATTRIBUTE_NAME=name_of_the_parameter_on_the_left
would be $WSRU or just WSRU?

Fabio L Pinto commented on March 7, 2016 Permalink
Hello CSTALKER,

For your questions:

1. If you have both scenarios 1 and 2 matching with your requestTest.jsp page, the second should be applied since more restrictive and complete for successful SSO implementation for your business;
2. you read on reqeustTest.jsp $WSRU that will mean HTTP variable in place (starting with $), but when updating your IBM TRIRIGAWEB.properties, you should enter : SSO_REQUEST_ATTRIBUTE_NAME=WSRU

See that SSO implementation (IBM TRIRIGA terminology) will mean challenging the Internet browser session for credential, meaning a pop-up login page will show up for user to enter domain credential. If you don't want this happening, it means you want Seamless Sign in , and IBM TRIRIGA will not implement or support it (this happens on other layers: WebServer & Application Server). See more information on that on :

- SSO Compatibility - https://www.ibm.com/developerworks/community/wikis/home?lang=en#!/wiki/IBM+TRIRIGA1/page/SSO+Compatibility

Hope this helps.

Thanks a lot.

Regards.

Fabio L Pinto commented on September 6, 2016 Permalink
Hello,

The SSO HTTP header user name field value must have a perfect match with IBM TRIRIGA user account value, but considering the following SSO attributes on TRIRIGAWEB.properties if avaialbe and set up:

USERNAME_CASE_SENSITIVE
SSO_REMOVE_DOMAIN_NAME

Think it needs to have a perfect match (considering the both SSO parameter on TRIRIGAWEB.properties file above), and think that the following SQL statement may help on this check-up:

select user_account from user_credentials where user_account like '%<HTTP header user name>%'

If this makes sense and it is true, may you kindly add this to the troubleshooting list above?

Thanks a lot.

Regards.

Edited on September 6, 2016

GiuCS commented on October 24, 2016 Permalink

Hi there,

It seems the $ for WSRU can be used depending on the webserver configuration, so for step 2 you can try both with $WSRU and WSRU to see how it goes.

Thank you.

deepsharma.951 commented on April 7, 2017 Permalink

i want to authenticate user through mobile using SSO also if we have token through local authenticate server so how could we authenticate token with TririgaWS object.

Edited on April 7, 2017

zhangke123 commented on September 6, 2018 Permalink

Does tririga support SP-Initiated web single sign-on (SSO) using SAML with other IDM system? if yes, how?

Show 10 | 25 | 50 items per page Previous | Next

Feed for this page | Feed for these comments