



IAM

WEB SSO Troubleshooting Guide

Version 12.0.18



Change Log

Date	Change Description
Nov 2, 2019	Version 12.0.18 document release.

CONTENT

Chapter 1 Confirm the environment deployment	1
Chapter 2 Common problem	1

Chapter 1 Confirm the environment deployment

1. The web server is in the internal network area of the IAM. Because the data does not pass through the IAM device when accessing the web server, the traffic needs to be mirrored to the IAM.
2. The web server is on the external network of IAM. At this time, the web login data passes through IAM. You only need to confirm that you can catch the correct login keywords.
3. Some data streams are going to special scenarios, such as when a PC accesses data from a web single sign-on server, first go to the exit router, and then return to the web single sign-on server. In this case, web single sign-on is unsuccessful.

Chapter 2 Common problem

1. The IP address of the Web authentication server cannot be filled in the global exclusion list of the IAM device. Adding IAM will not process the data of the Web authentication server.
2. If the web server address is in the form of IP or IP: port, you must also select " Before authentication, added to group(Users accessing any HTTP content must be authenticated)" in other authentication options, and confirm the policy permissions of the root group. Pass the data of this IP and port.

The screenshot shows the 'Single Sign-On(SSO)' configuration page for the 'Web' category. The left sidebar lists various categories, with 'Web' selected. The main configuration area includes the following settings:

- Category:** Web
- Enable Web SSO:** ☒
- Web Authentication Server:** 120.193.35.247:8001/web/wzct/login.seam
- Type:** Form submitted using POST
- User Form Name:** Form1%3AtxtUserName
- Authentication Succeeds/Fails Upon Keyword Matching:**
 - ☒ Authentication success keywords: success
 - ☐ Authentication failure keywords:

3. The user form name needs to be completed. Through packet capture analysis, the fields before the user name are taken until the ampersand, and the user name field is looked forward to the ampersand. As shown below:

```
Stream Content
POST /web/wzct/login.seam HTTP/1.1
x-requested-with: XMLHttpRequest
Accept-Language: zh-cn
Referer: http://120.193.35.247:8001/web/wzct/login.seam
Accept: application/xml, text/xml, */*
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET CLR 2.0.50727; InfoPath.3)
Host: 120.193.35.247:8001
Content-Length: 172
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: JSESSIONID=43666A784C7D9A9060BC6E9E9ECA0FBB
Form1=Form1&Form1%3AtxtUserName=admin&Form1%3AtxtPwd=wz1234&javax.faces.ViewState=j_3Aj_id18&primefacesPartialRequest=true&frameType=&Form1:j_id6_ajax=Form1:j_id6_ajaxH
200 OK
Server: Apache-Coyote/1.1
X-Powered-By: Servlet 2.4; JBoss-4.2.3.GA (build: SVNTag=JBoss_4_2_3_GA date=2008071
JBossWeb-2.0
X-Powered-By: JSF/1.2
Cache-Control: no-cache, must-revalidate, max-age=0, no-store
```

4. The authentication method using WEB single sign-on is used, but the obtained user name is abnormal, as shown below:

Members			
<input type="checkbox"/>	No.	Username(Alias)	Group
<input type="checkbox"/>	1	testgu; jsessionid=e80246bacbdcd292b6a331eaf9f4cbb username=testgu-[temp]	/...

Capture the authenticated data packet and view the contents of the post data packet. The data packet screenshot is as follows:

```
POST / HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Referer: http://10.10.10.88/
Accept-Language: zh-Hans,en-US;q=0.7,en;q=0.3
User-Agent: Mozilla/5.0 (MSIE 8.0; windows NT 6.3; WOW64; Trident/7.0; rv:11.0) like Gecko
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
Host: 10.10.10.88
Content-Length: 48
DNT: 1
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: username=testgu; JSESSIONID=31545FAEE7E433A816F5A82CEFE2825E

username=testgu&password=ztol23456imm&checkbox=1HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Content-Encoding: gzip
Vary: Accept-Encoding
Date: Thu, 21 Aug 2014 09:55:01 GMT
```

The theory of WEB single sign-on to obtain a user name is:

After detecting the user form name (username in this example), the content behind the form name will be intercepted as the user name, and the detected ampersand will end.

The user name will not only detect the content of the http post data packet, but also the cookie content when the data packet contains a cookie.

Through the data package, you can see that the upload has a cookie, and the cookie has the username form name, but the form name does not end with an ampersand, but ends with a semicolon. Because the device cannot recognize the end character, continue to the next until the ampersand in the post content is matched. So we see that long list of usernames in the online user list.

[Solution]: This problem is that the client's web server does not meet our standards. It is recommended that the client change the terminator of the form name in the cookie to an ampersand.

3. if encounter unsuccessful web single sign-on and confirm that there are no problems with successful keywords and configuration. You can test with: symbols and; symbols as keywords to test, because general web page posts will be included, if it still does not work, you can type debug logs and Capture

and analyze the data packets, and confirm that there is no problem, if the problem still exist, you can feedback to the R&D there.



SANGFOR

Copyright © SANGFOR Technologies Inc. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of SANGFOR Technologies Inc.

SANGFOR is the trademark of SANGFOR Technologies Inc. All other trademarks and trade names mentioned in this document are the property of their respective holders.

Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied. The information in this document is subject to change without notice. To obtain the latest version, contact the international service center of SANGFOR Technologies Inc