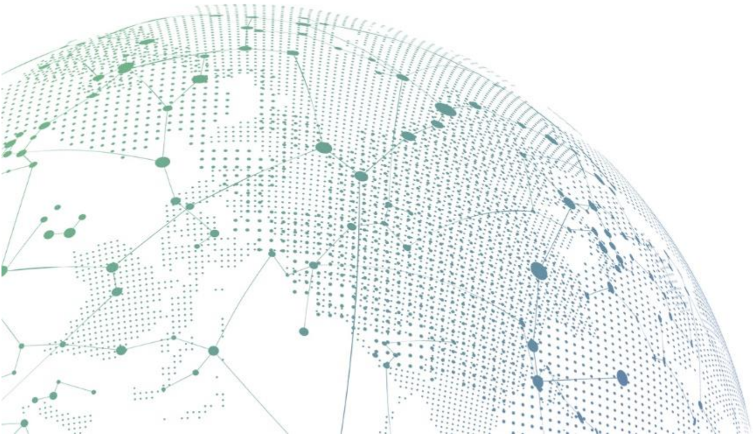
SANGFOR

IAM

Web Single Sign-On Configuration Guide

Version 12.0.18



Change Log

Date	Change Description
Dec 31, 2019	Version 12.0.18 document release.

CONTENT

Chapter 1 Content requirements 1

1 Product Introduction 1

2 Application Scenario 1

3 Requirement Condition 1

4 Configuration Idea 1

5 Configuration Guide with Screenshot 1

5.1 Testing environment and requirement 1

5.2 Single Sign-On configuration 1

5.3 Authentication policy configuration 3

6 Precaution 3

Chapter 1 Content requirements

1 Product Introduction

While user login with their own web application, at the same time the user will login on our device with their business system username.

2 Application Scenario

1. Our devices as customer authentication system. Customer with their own web system to allow user for login at the same time login on our device as authenticate user to access internet.

2. Client has their own web authentication system with username and password system, to achieve after perform web authentication do not need to relogin on our device with submit the username and identify the identity on our device for internet access.

3 Requirement Condition

1. IAM device with version 12.0.18 or above
2. A web login system with data passing through our device

4 Configuration Idea

1. Prepare a testing environment.
2. Configure a Single Sign-On
3. Configure an authentication policy.

5 Configuration Guide with Screenshot

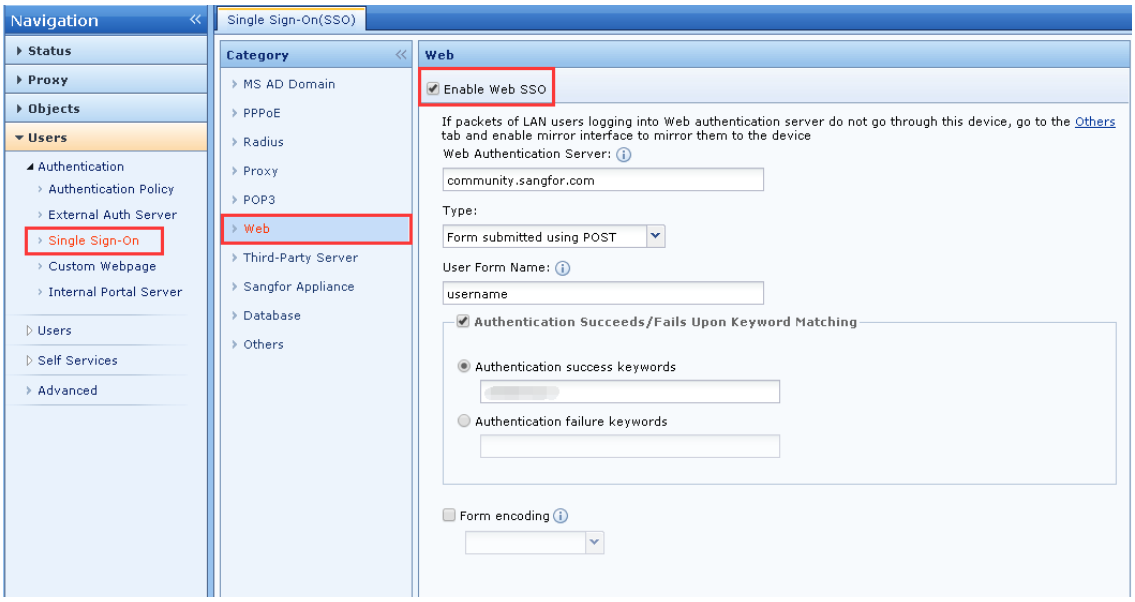
5.1 Testing environment and requirement

Before implement the web single sign-on, we must understand the client network environment which whether the web system traffic will pass through our device. Configure a web single sign-on if the traffic pass through our device, else if the traffic do not pass through our device, we need to redirect the corresponding data to our device.

5.2 Single Sign-On configuration

IAM 11.0 web single sign-on has major changes compared to previous versions. In addition supported POST submit username function, it added the function of taking user data through cookie and URL parameter. We will select the [Type] that to be related to the way that user summit the username on the web application. We can determine whether the user login is successful based on the return value of the server. We unable to identify whether the login was successful if no response from the server.

Diagram below is the Single Sign-On configuration by POST submit as example,



☑ Enable Web SSO

If packets of LAN users logging into Web authentication server do not go through this device, go to the Others tab and enable mirror interface to mirror them to the device

Web Authentication Server: community.sangfor.com

Type: Form submitted using POST

User Form Name: username

☑ Authentication Succeeds/Fails Upon Keyword Matching

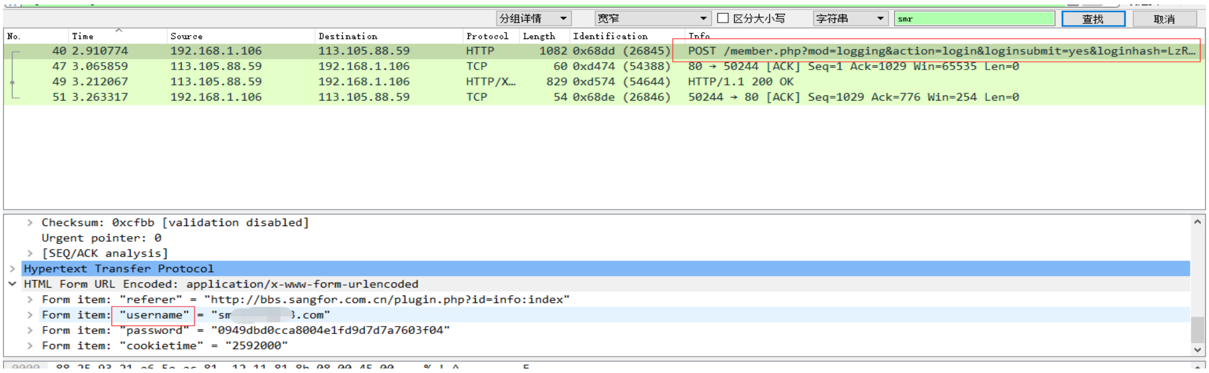
● Authentication success keywords [redacted]

○ Authentication failure keywords

□ Form encoding

Web authentication server fill in with user web domain name or ip address, as diagram above fill in with community.sangfor.com, select the [Type] as form submitted using POST, fill in the [User Form Name:] based on the actual form name, you may look for the web admin to provide the information, else you may use httpswatch for wireshark to capture the traffic packet to identify the needed information.

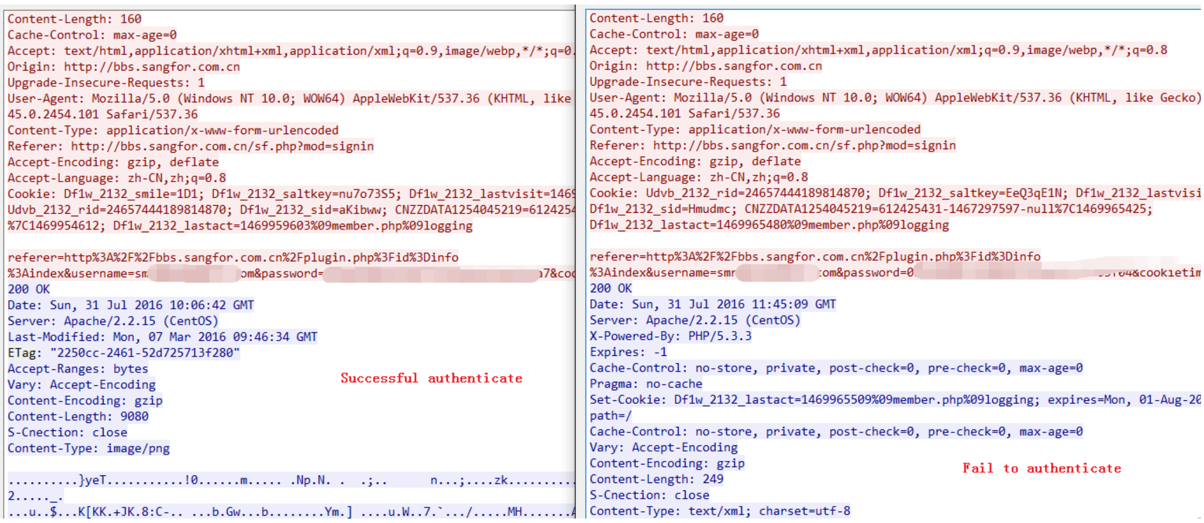
By capturing the packet from “community.sangfor.com” as diagram below, we able to see the username from the form name is “Username”.



```
No.   Time       Source          Destination     Protocol Length Identification  Info
   40 2.910774   192.168.1.106   113.105.88.59   HTTP      1082 0x68dd (26845)  POST /member.php?mod=logging&action=login&loginsubmit=yes&loginhash=LzR…
   47 3.065859   113.105.88.59   192.168.1.106   TCP         60 0xd474 (54388)  80 → 50244 [ACK] Seq=1 Ack=1029 Win=65535 Len=0
   49 3.212067   113.105.88.59   192.168.1.106   HTTP/X…    829 0xd574 (54644)  HTTP/1.1 200 OK
   51 3.263317   192.168.1.106   113.105.88.59   TCP         54 0x68de (26846)  50244 → 80 [ACK] Seq=1029 Ack=776 Win=254 Len=0
```

```
  > Checksum: 0xcfbb [validation disabled]
    Urgent pointer: 0
  > [SEQ/ACK analysis]
> Hypertext Transfer Protocol
v HTML Form URL Encoded: application/x-www-form-urlencoded
  > Form item: "referer" = "http://bbs.sangfor.com.cn/plugin.php?id=info:index"
  > Form item: "username" = "sm[redacted]3.com"
  > Form item: "password" = "0949dbd0cca8004e1fd9d7d7a7603f04"
  > Form item: "cookietime" = "2592000"
```

The following is enable the [Authentication keyword], here you able to choose the success keyword or the failure keyword. You may get the keyword from the returned data by the web server. As the diagram below is the packet capture by wireshark and compare the successful authenticate and fail to authenticate data that returned by server.


Successful authenticate

```
Content-Length: 160
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.
Origin: http://bbs.sangfor.com.cn
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like
45.0.2454.101 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Referer: http://bbs.sangfor.com.cn/sf.php?mod=signin
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.8
Cookie: Df1w_2132_smile=1D1; Df1w_2132_saltkey=nu7o73S5; Df1w_2132_lastvisit=146
Udvb_2132_rid=246574441898148 70; Df1w_2132_sid=aKibww; CNZZDATA1254045219=612425
%7C1469954612; Df1w_2132_lastact=1469959603%09member.php%09logging

referer=http%3A%2F%2Fbbs.sangfor.com.cn%2Fplugin.php%3Fid%3Dinfo
%3Aindex&username=sm[redacted]om&password=[redacted]a7&co
200 OK
Date: Sun, 31 Jul 2016 10:06:42 GMT
Server: Apache/2.2.15 (CentOS)
Last-Modified: Mon, 07 Mar 2016 09:46:34 GMT
ETag: "2250cc-2461-52d725713f280"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 9080
S-Cnection: close
Content-Type: image/png

..........}yeT...........!0......m..... .Np.N. .  .;..      n...;....zk.........
2....._.
...u..$...K[KK.+JK.8:C-.. ...b.Gw...b........Ym.] ....u.W..7.`.../.....MH.......
```

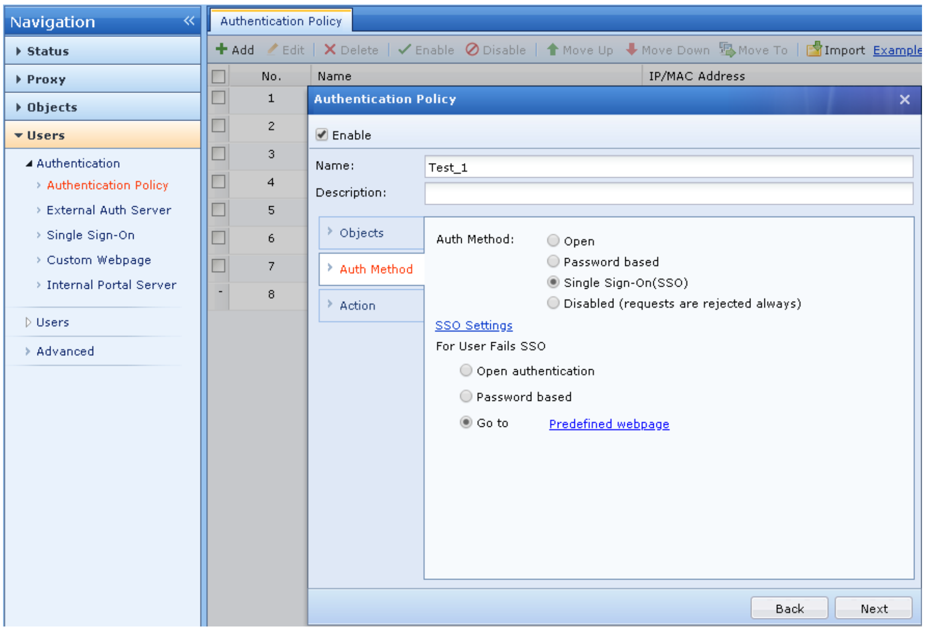
Fail to authenticate

```
Content-Length: 160
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Origin: http://bbs.sangfor.com.cn
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
45.0.2454.101 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Referer: http://bbs.sangfor.com.cn/sf.php?mod=signin
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.8
Cookie: Udvb_2132_rid=24657444189814870; Df1w_2132_saltkey=EeQ3qE1N; Df1w_2132_lastvisi
Df1w_2132_sid=Hmudmc; CNZZDATA1254045219=612425431-1467297597-null%7C1469965425;
Df1w_2132_lastact=1469965480%09member.php%09logging

referer=http%3A%2F%2Fbbs.sangfor.com.cn%2Fplugin.php%3Fid%3Dinfo
%3Aindex&username=smr[redacted]om&password=0[redacted]&cookietim
200 OK
Date: Sun, 31 Jul 2016 11:45:09 GMT
Server: Apache/2.2.15 (CentOS)
X-Powered-By: PHP/5.3.3
Expires: -1
Cache-Control: no-store, private, post-check=0, pre-check=0, max-age=0
Pragma: no-cache
Set-Cookie: Df1w_2132_lastact=1469965509%09member.php%09logging; expires=Mon, 01-Aug-20
path=/
Cache-Control: no-store, private, post-check=0, pre-check=0, max-age=0
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 249
S-Cnection: close
Content-Type: text/xml; charset=utf-8
```

5.3 Authentication policy configuration

For the authentication policy, ensure that understand the authenticate object before configure the policy, select [Single Sign-On] as the authentication method, for user fails SSO can be configure according to customer needs as the diagram below.



Authentication Policy

☑ Enable

Name: Test_1

Description:

Auth Method: ○ Open ○ Password based ● Single Sign-On(SSO) ○ Disabled (requests are rejected always)

SSO Settings

For User Fails SSO

○ Open authentication

○ Password based

● Go to Predefined webpage

6 Precaution

1. During the testing, do not perform repeated login and logout operations on an IP address, it will cause fail SSO authenticate.
2. The way that we mention to obtain the "username" for the form table and the authenticate keyword is using httpwatch and wireshark, from this document we do not provide the operating guide and you may find out the operation method by yourself.

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