



IAM

Open Authentication Troubleshooting Guide

Version 12.0.18



Change Log

Date	Change Description
May 30, 2019	Version 12.0.18 document release.

CONTENT

Chapter 1 Use Open Authentication but no users in Oline Users	1
---	---

Chapter 1 Use Open Authentication but no users in Online Users

- Check if there is a test ip connection on the IAM and if the traffic is bidirectional.

Connections							
Search by IP Address 192.168.19.217							
No.	Username(Alias)	Group	Source	Destination	Protocol	App Category	Application
9	192.168.19.217	/	192.168.19.217:49209	14.215.138.61:443	TCP	NET Protocol	SSL
10	192.168.19.217	/	192.168.19.217:49205	172.217.24.174:443	TCP	NET Protocol	SSL
11	192.168.19.217	/	192.168.19.217:49181	172.217.31.36:443	TCP	NET Protocol	SSL
12	192.168.19.217	/	192.168.19.217:49182	172.217.31.42:443	TCP	NET Protocol	SSL
13	192.168.19.217	/	192.168.19.217:49185	172.217.31.99:443	TCP	NET Protocol	SSL
14	192.168.19.217	/	192.168.19.217:49179	172.217.31.99:443	TCP	NET Protocol	SSL
15	192.168.19.217	/	192.168.19.217:49203	203.205.128.137:443	TCP	NET Protocol	SSL
16	192.168.19.217	/	192.168.19.217:49204	203.205.128.173:443	TCP	NET Protocol	SSL
17	192.168.19.217	/	192.168.19.217:49207	203.205.128.175:443	TCP	NET Protocol	SSL
18	192.168.19.217	/	192.168.19.217:49206	203.205.128.175:443	TCP	NET Protocol	SSL
19	192.168.19.217	/	192.168.19.217:49200	203.205.138.57:443	TCP	NET Protocol	SSL

- Check whether the data packet has a TCP protocol packet, and there is no TCP protocol packet. Then, if Open Authentication is configured, the IP of the PC will not appear in **Online Users**.

No.	Time	Source	Destination	Protocol	Length	Source Port	Destination Port	Time to live	Info
372	15:06:00.794466	192.168.19.217	216.58.196.42	TCP	60	49246	443	128	49246 → 443 [SYN] Seq=0 Win=0 Len=0 MSS=1460 WS=256 SACK_PERM=1
374	15:06:00.814461	216.58.196.42	192.168.19.217	TCP	66	443	49246	123	443 → 49246 [SYN, ACK] Seq=0 Ack=1 Min=60720 Len=0 MSS=1380 SACK_PERM=1 WS=256
375	15:06:00.818057	192.168.19.217	216.58.196.42	TCP	54	49246	443	128	49246 → 443 [ACK] Seq=1 Ack=1 Min=131072 Len=0
376	15:06:00.819212	192.168.19.217	216.58.196.42	TLSv1.3	571	49246	443	128	Client Hello
413	15:06:00.838902	216.58.196.42	192.168.19.217	TCP	60	443	49246	123	443 → 49246 [ACK] Seq=1 Ack=518 Min=61952 Len=0
414	15:06:00.846320	216.58.196.42	192.168.19.217	TLSv1.3	1484	443	49246	123	Server Hello, Change Cipher Spec
415	15:06:00.846664	216.58.196.42	192.168.19.217	TCP	1484	443	49246	123	443 → 49246 [ACK] Seq=1431 Ack=518 Min=61952 Len=1430 [TCP segment of a reassembled PDU]
416	15:06:00.846733	192.168.19.217	216.58.196.42	TCP	54	49246	443	128	49246 → 443 [ACK] Seq=518 Ack=2861 Min=131072 Len=0
417	15:06:00.848203	216.58.196.42	192.168.19.217	TLSv1.3	1113	443	49246	123	Application Data
427	15:06:00.854809	192.168.19.217	216.58.196.42	TLSv1.3	118	49246	443	128	Change Cipher Spec, Application Data
428	15:06:00.855653	192.168.19.217	216.58.196.42	TLSv1.3	140	49246	443	128	Application Data
429	15:06:00.855654	192.168.19.217	216.58.196.42	TLSv1.3	283	49246	443	123	Application Data
430	15:06:00.875091	216.58.196.42	192.168.19.217	TLSv1.3	618	443	49246	123	Application Data, Application Data
431	15:06:00.875798	192.168.19.217	216.58.196.42	TLSv1.3	85	49246	443	128	Application Data

- Check whether there is a multi-layer protocol encapsulation, such as QinQ protocol encapsulation. If there is a protocol such as QinQ, you need to enable "**Protocol Extension**".

Protocol Extension

☒ Enable protocol stripping ⓘ

Protocol	
<input type="checkbox"/> Name	Port(applied to L3 protocol only)
<input checked="" type="checkbox"/> VLAN(Q-in-Q) de-encapsulation	-
<input type="checkbox"/> MPLS de-encapsulation	-
<input type="checkbox"/> PPPoE de-encapsulation	-
<input type="checkbox"/> L2TP de-encapsulation	1701
<input type="checkbox"/> LWAPP de-encapsulation	12222
<input type="checkbox"/> CAPWAP de-encapsulation	5247
<input type="checkbox"/> WLTP de-encapsulation	6969,7070
<input type="checkbox"/> Custom protocol de-encapsulatio	-

Custom Protocol Stripping ⓘ

Ethernet Header: Offset bytes away from Ethernet header
 Feature value is

IP Header Start Position: Offset bytes away from Ethernet header

Commit

- If it is bypass mode, you need to check whether the IP address segment in Listened and Excluded IP Addresses is complete.

Mirror Port:

Listened and Excluded IP Addresses

IP Addresses: One IP address or range per row;
 Listened subnet examples: 200.200.20.0/255.255.255.0, 2001:4008::/64
 Excluded IP address or range begins with hyphen. Excluded IP range examples:
 -200.200.20.14-200.200.20.148, -2001:4008::1-2001:4008::ffff; Excluded IP
 address examples: -200.200.20.58, -2001:4008::1

- Check if you have made the wrong IP/MAC binding, or turn on **Troubleshooting** to check for a drop log.

IP&MAC Binding			
<div> Add Delete Select Import Export Example File </div> <div> Search by IP Address Search </div>			
IP Address	MAC Address	Description	Delete
<input type="checkbox"/> 192.168.19.217	ee-fe-fc-ed-ee-ee		<input checked="" type="checkbox"/>

No.	Time	Src IP→Dest IP	Protocol	Data Flow	eth0 → NULL	Size	Line	Line	Application	Rule	Source	Packet Drop	Action
						Sum	SSL	SSL					
18	15:23:05	192.168.19.217→108.144.3 → 192.108.19.217	tcp	eth0 → NULL	105(B)	105(B)	Line1	SSL	SSL_Shello	authv	web authn	DROPPFLAG	(line:738)this packet had been dropped by authv!
19	15:25:05	192.168.19.217→49367 → 125.39.83.1	tcp	eth0 → NULL	105(B)	105(B)	Line1	SSL	SSL_Shello	authv	web authn	DROPPFLAG	User blocked(after code)
20	15:25:05	192.168.19.217→49367 → 125.39.83.1	tcp	eth0 → NULL	105(B)	105(B)	Line1	SSL	SSL_Shello	authv	web authn	DROPPFLAG	User blocked(after code)
21	15:25:05	125.39.83.108→443 → 192.168.19.217	tcp	eth0 → NULL	206(B)	206(B)	Line1	SSL	SSL_Shello	authv	web authn	DROPPFLAG	User blocked(after code)
22	15:25:05	192.168.19.217→49366 → 125.39.83.1	tcp	eth0 → NULL	87(B)	87(B)	Line1	SSL	TLS_Cv1	web authn	web authn	DROPPFLAG	(line:738)this packet had been dropped by authv!
23	15:25:05	192.168.19.217→49366 → 125.39.83.1	tcp	eth0 → NULL	87(B)	87(B)	Line1	SSL	TLS_Cv1	authv	web authn	DROPPFLAG	User blocked(after code)
24	15:25:05	192.168.19.217→49366 → 125.39.83.1	tcp	eth0 → NULL	105(B)	105(B)	Line1	SSL	SSL_Shello	web authn	web authn	DROPPFLAG	(line:738)this packet had been dropped by authv!
25	15:25:05	192.168.19.217→49366 → 125.39.83.1	tcp	eth0 → NULL	105(B)	105(B)	Line1	SSL	SSL_Shello	authv	web authn	DROPPFLAG	User blocked(after code)
26	15:25:05	125.39.83.108→443 → 192.168.19.217	tcp	eth2 → NULL	206(B)	206(B)	Line1	SSL	SSL_Shello	authv	web authn	DROPPFLAG	User blocked(after code)
27	15:25:05	192.168.19.217→49365 → 125.39.83.1	tcp	eth0 → eth2	87(B)	87(B)	Line1	SSL	TLS_Cv1	web authn	web authn	DROPPFLAG	(line:738)this packet had been dropped by authv!
28	15:25:05	192.168.19.217→49365 → 125.39.83.1	tcp	eth0 → NULL	87(B)	87(B)	Line1	SSL	TLS_Cv1	authv	web authn	DROPPFLAG	User blocked(after code)
29	15:25:05	192.168.19.217→49365 → 125.39.83.1	tcp	eth0 → eth2	105(B)	105(B)	Line1	SSL	SSL_Shello	web authn	web authn	DROPPFLAG	(line:738)this packet had been dropped by authv!
30	15:25:05	192.168.19.217→49365 → 125.39.83.1	tcp	eth0 → NULL	105(B)	105(B)	Line1	SSL	SSL_Shello	authv	web authn	DROPPFLAG	User blocked(after code)
31	15:25:05	125.39.83.108→443 → 192.168.19.217	tcp	eth2 → NULL	206(B)	206(B)	Line1	SSL	SSL_Shello	authv	web authn	DROPPFLAG	User blocked(after code)
32	15:25:05	192.168.19.217→49367 → 125.39.83.1	tcp	eth0 → NULL	571(B)	571(B)	Line1	SSL	SSL_Chello	authv	web authn	DROPPFLAG	User blocked(after code)
33	15:25:05	192.168.19.217→49367 → 125.39.83.1	tcp	eth0 → NULL	54(B)	54(B)	Line1	0	0	authv	web authn	DROPPFLAG	User policy logic(AcCode) dropped ssl
34	15:25:05	192.168.19.217→49366 → 125.39.83.1	tcp	eth0 → NULL	571(B)	571(B)	Line1	SSL	SSL_Chello	authv	web authn	DROPPFLAG	User blocked(after code)

- Global Exclusion

Predefined Excluded Address

Custom Excluded Address

+ Add

✓ Enable

⊘ Disable

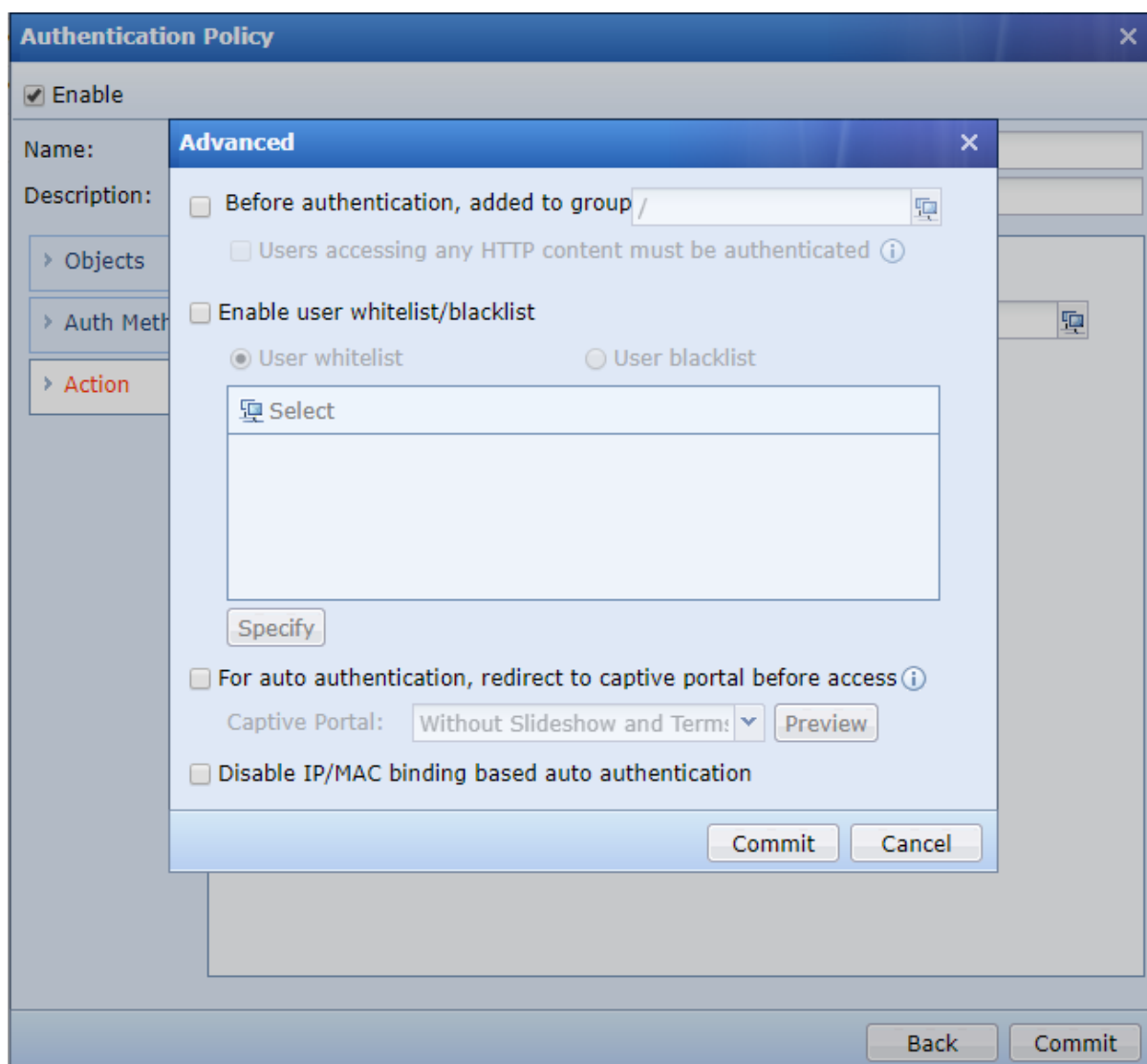
✗ Delete

Search:

<input type="checkbox"/>	Address	Description	Status	Delete
<input type="checkbox"/>	192.200.19.81		✓	✗

Commit

- W.: www.sangfor.com | W.: community.sangfor.com | E.: tech.support@sangfor.com



- Devices deployed in bridge mode need to check whether the network cable is reversed. If the network cable is connected and the **"Open auth for data flow from WAN to LAN interface"** is enabled, the IP of the intranet may not be online.

Other Options

- ☒ DNS service is available even user is not authenticated or is locked
- ☒ Redirect HTTPS requests(not using proxy) to captive portal if user is not authenticated ⓘ
- ☐ For Internet access using proxy, password submission is Web based
- ☒ Username of domain user is domain account plus domain name
- ☒ **Open auth for data flow from WAN to LAN interface**
- ☐ Disable sorting by user/group ⓘ



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