



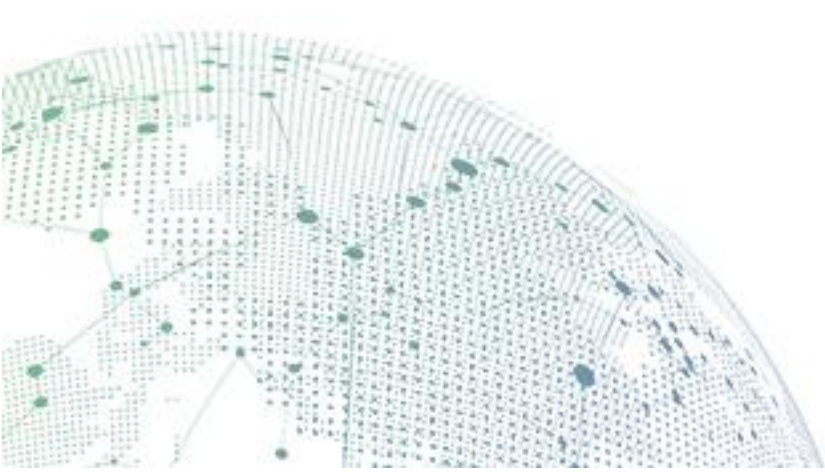
SANGFOR



IAM

Radius SSO POC Guide

Version 12.0.13



Change Log

Date	Change Description

CONTENT

Chapter 1 Background requirement	4
Chapter 2 Implementation method.....	4
2.1 Preparation	4
Chapter 3 Testing environment.....	4
3.1 Testing topology.....	4
3.2 Configuration	5
Chapter 4 Testing procedure.....	6
Chapter 5 Testing result.....	7
Chapter 6 Precautions	7

Chapter 1 Background requirement

【Description】 : When customer login into third party authentication server such as Radius, IAM should able retrieve username and IP for SSO automatically.

Chapter 2 Implementation method

2.1 Preparation

1. One unit IAM 11.0 as testing device and deploy in route mode.
2. Radius's authenticated traffic does not flow through IAM, so require configure mirror port in switch to mirror the traffic.

II. Testing requirements and expected results

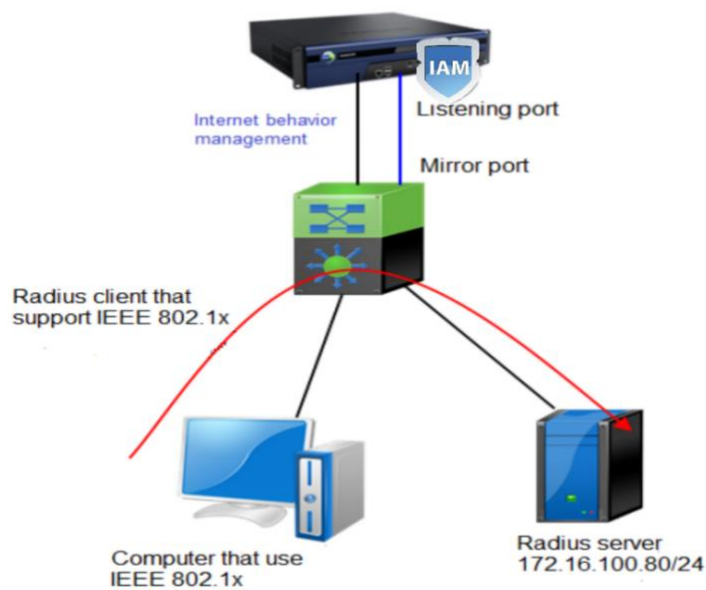
PC pass Radius authentication that means it also pass IAM authentication. The online users list of IAM able to view authenticated accounts and IP.

III. Deployment

Authentication and auditing is perform by third party authentication server, Radius. IAM as routing gateway, the Radius's authenticated traffic does not flow through IAM. IAM need to configure mirror port and Radius single sign-on, so that the Radius's authenticated traffic can mirror to IAM mirror port.

Chapter 3 Testing environment

3.1 Testing topology



3.2 Configuration

1. Basic network configuration

【Network】 — 【Deployment】 Configure the deployment mode of device as route mode. Besides, configure WAN interface IP, LAN interface IP, DNS and NAT.

2. Configure authentication policy

【Authentication】 - 【User Authentication】 - 【Authentication Policy】 Configure authentication policy for internal network as open authentication or single sign-on (SSO).

3. Radius Configuration

【Authentication】 - 【Single Sign-On】 - 【Radius】 Insert Radius server IP address and authentication port.

The screenshot shows the Sangfor IAM11.0 web interface. The navigation menu on the left is expanded to 'Authentication' > 'Single Sign-On'. The 'RADIUS' configuration page is displayed, with the 'RADIUS' option highlighted in the 'Category' list. The 'RADIUS' section is checked, and the 'RADIUS Server Addresses' table is visible. A red box highlights the format instructions and the first two rows of data in the table.

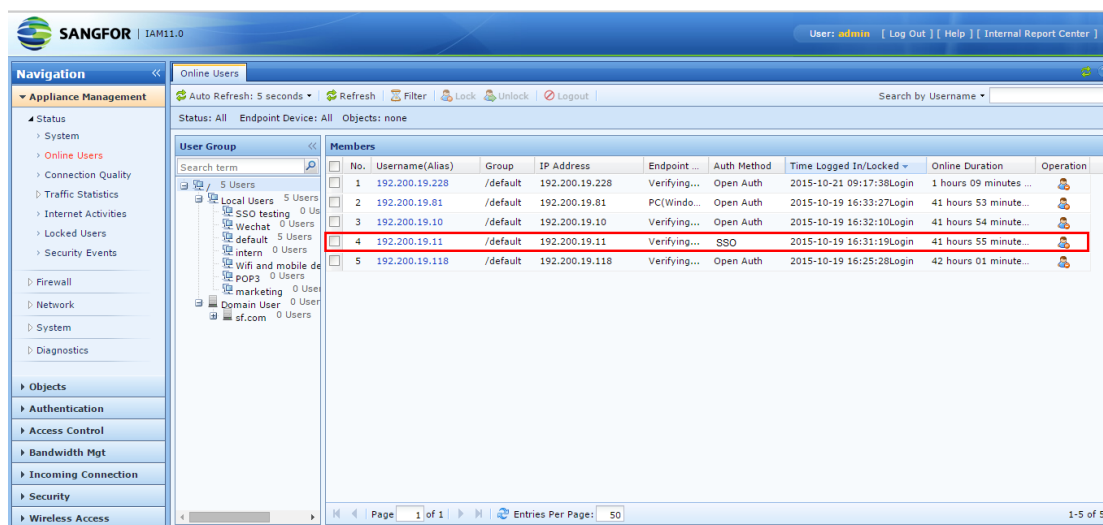
RADIUS Server Addresses
192.168.0.1
192.168.0.1:1813
2001::1
[2001::1]:1813

Description: Insert Radius server IP and port which is 1813 by default in RADIUS Server Addresses table.

Chapter 4 Testing procedure

1. PC open 802.1x client and insert accounts password for authenticated.
2. If IAM able listen authenticated Authentication Request, this means users can online.

Chapter 5 Testing result



The screenshot displays the SANGFOR IAM11.0 Online Users interface. The left sidebar shows the navigation menu with 'Online Users' selected. The main area shows a table of active users with the following data:

No.	Username(Alias)	Group	IP Address	Endpoint...	Auth Method	Time Logged In/Locked	Online Duration	Operation
1	192.200.19.228	/default	192.200.19.228	Verifying...	Open Auth	2015-10-21 09:17:38Login	1 hours 09 minutes ...	
2	192.200.19.01	/default	192.200.19.01	PC(Windo...	Open Auth	2015-10-19 16:33:27Login	41 hours 53 minute...	
3	192.200.19.10	/default	192.200.19.10	Verifying...	Open Auth	2015-10-19 16:32:10Login	41 hours 54 minute...	
4	192.200.19.11	/default	192.200.19.11	Verifying...	SSO	2015-10-19 16:31:19Login	41 hours 55 minute...	
5	192.200.19.118	/default	192.200.19.118	Verifying...	Open Auth	2015-10-19 16:25:28Login	42 hours 01 minute...	

Chapter 6 Precautions

1. Radius Single Sign-On mainly use for third-party authentication, Radius environments. If IAM able to synchronize third party authentication Radius server, then use third party password authentication method.
2. IAM support route, bridge and bypass mode deployment. As long as the traffic is authenticated or auditing traffic, the traffic can listen by IAM. If authenticated or auditing traffic have flow through IAM, IAM does not need to configure listening port.



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