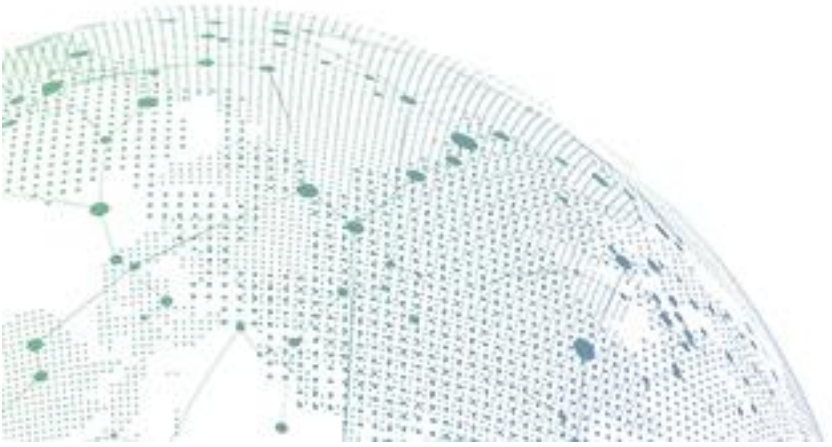
SANGFOR

IAM

Radius SSO POC Guide

Version 12.0.13



Change Log

Date	Change Description

CONTENT

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

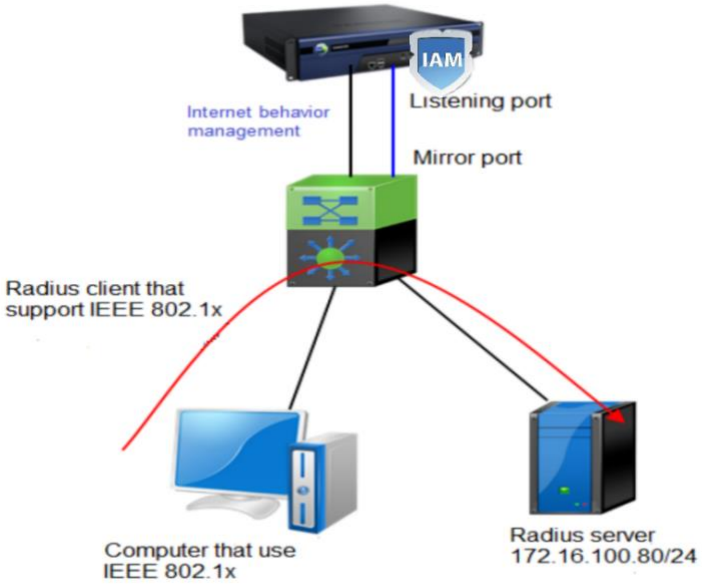
PC pass Radius authentication that means it also pass IAM authentication. The online users list of IAM able to view authenticated accounts and IP.

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

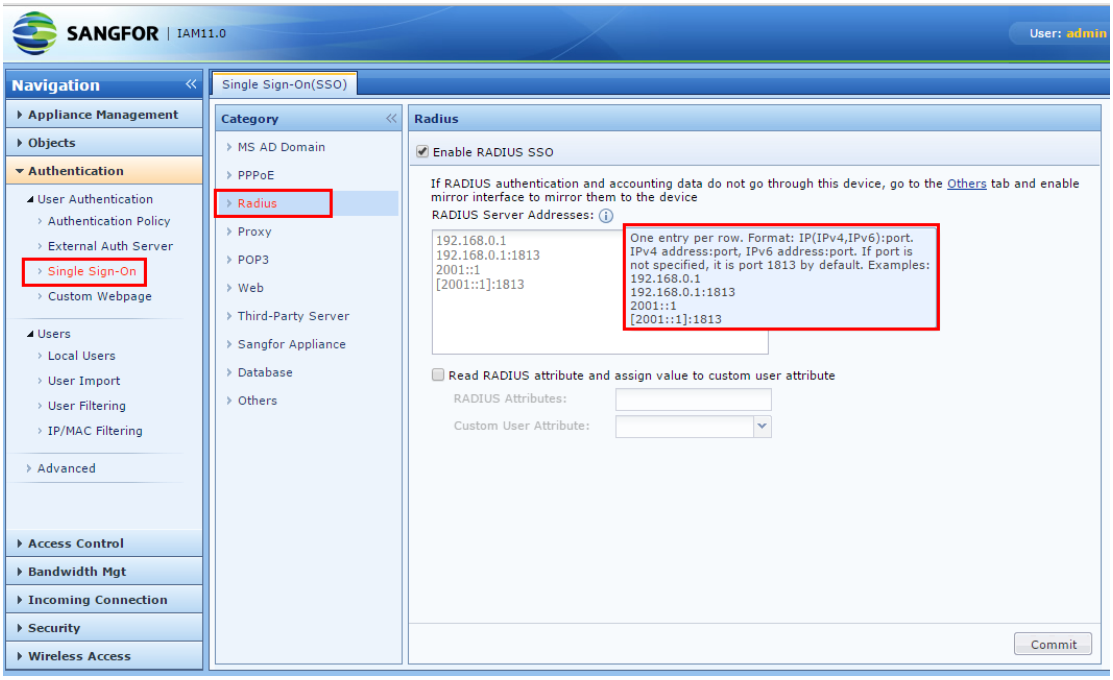
【Network】—【Deployment】Configure the deployment mode of device as route mode. Besides, configure WAN interface IP, LAN interface IP, DNS and NAT.

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.



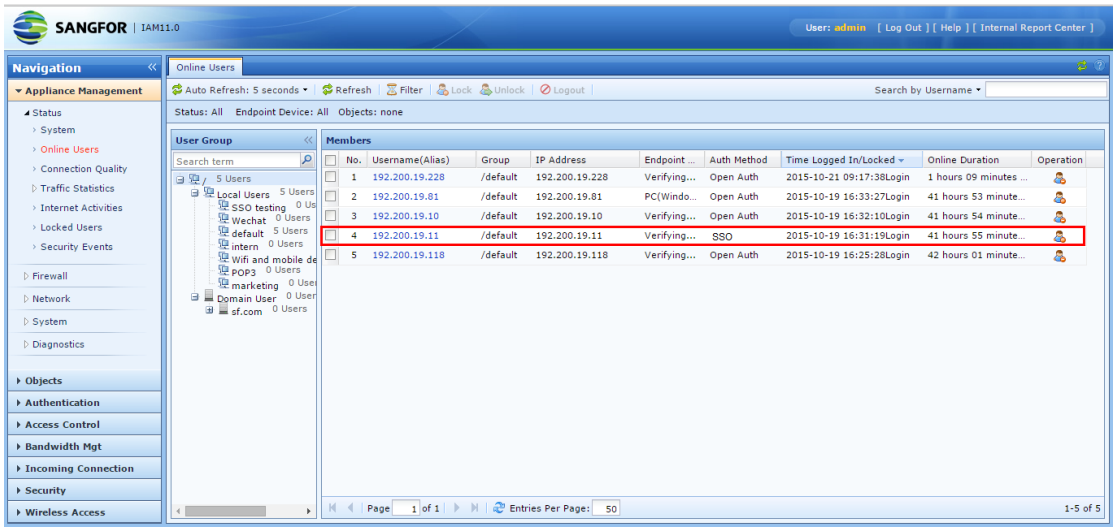
Description: Insert Radius server IP and port which is 1813 by default in RADIUS Server Addresses table.

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



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.

SANGFOR