IAM

Best Practices for Scenarios_Radius SSO

Version 12.0.42

Change Log

Date	Change Description
August 26, 2020	Version 12.0.42 document release.
May 17, 2021	Version 12.0.42 document update.

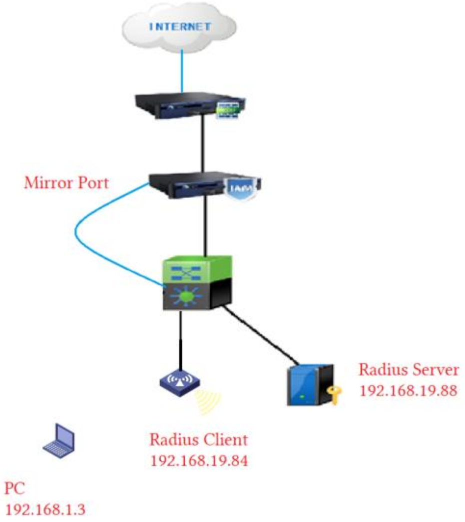
CONTENT

Chapter 1 Scenario

Radius is the abbreviation of Remote Authentication Dial. Radius was originally designed to authenticate and charge dial-up users. These functions are often used by telecommunications departments. The bills we receive after dial-up Internet access are counted by the Radius server. After using Radius for a period of time, everyone found that the Radius protocol is powerful, easy to use and easy to expand. Therefore, after improvements, Radius has now become an internationally accepted authentication billing protocol, which is widely used in ordinary telephone Internet access, ADSL Internet access, community broadband Internet access, Many occasions such as IP telephone.

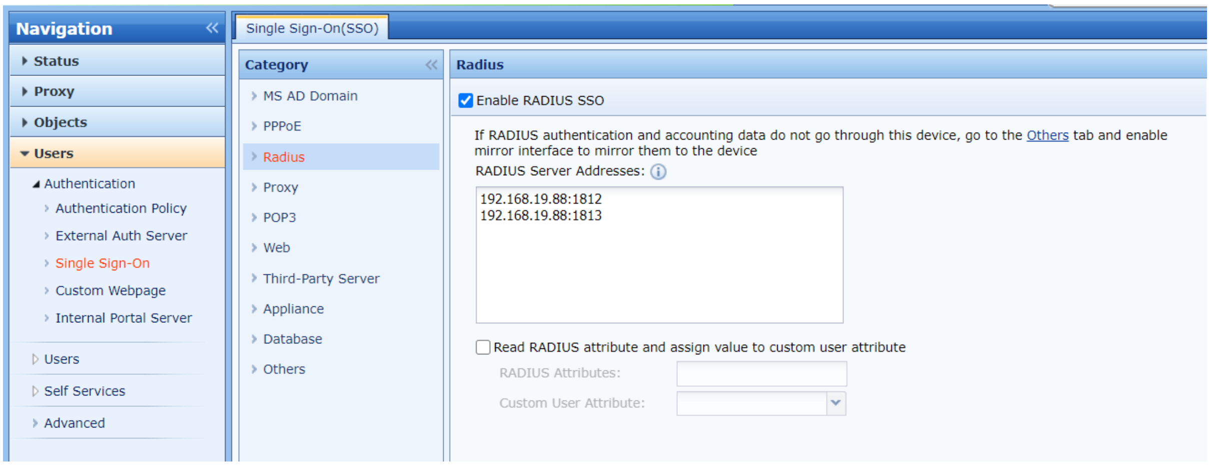
A large factory uses commercial wireless to allow employees to access the Internet, while using IAM to manage and audit users' online activity. At the authentication level, the IT department hopes to authenticate users in order to better manage the network. User names and passwords will be added to the Radius Server of the intranet when employees enter the company. The IT department hopes that users who have passed radius authentication do not need to pass IAM's secondary authentication.

Generally, the endpoint does not communicate directly with the Radius Server, but communicates with the Radius Client. For example, the wireless access controller here acts as the Radius Client.



Chapter 2 Configure IAM

1. Configure Radius SSO, you must specify the address and port of the Radius Server. The default ports are 1812 and 1813. If it is Cisco's Radius Server, the default ports are 1645 and 1646.



☑ Enable RADIUS SSO

If RADIUS authentication and accounting data do not go through this device, go to the Others tab and enable mirror interface to mirror them to the device

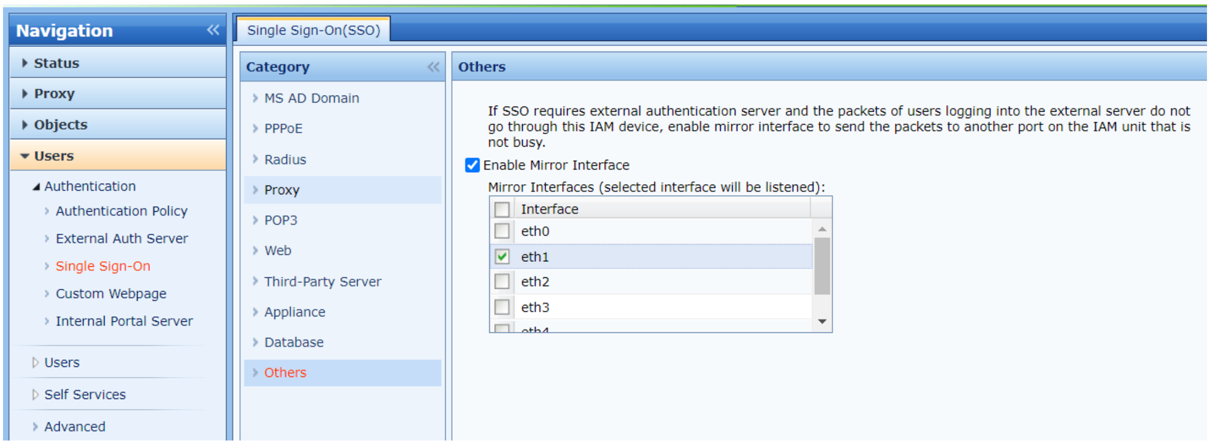
RADIUS Server Addresses:

192.168.19.88:1812
192.168.19.88:1813

☐ Read RADIUS attribute and assign value to custom user attribute

RADIUS Attributes:

Custom User Attribute:



Others

If SSO requires external authentication server and the packets of users logging into the external server do not go through this IAM device, enable mirror interface to send the packets to another port on the IAM unit that is not busy.

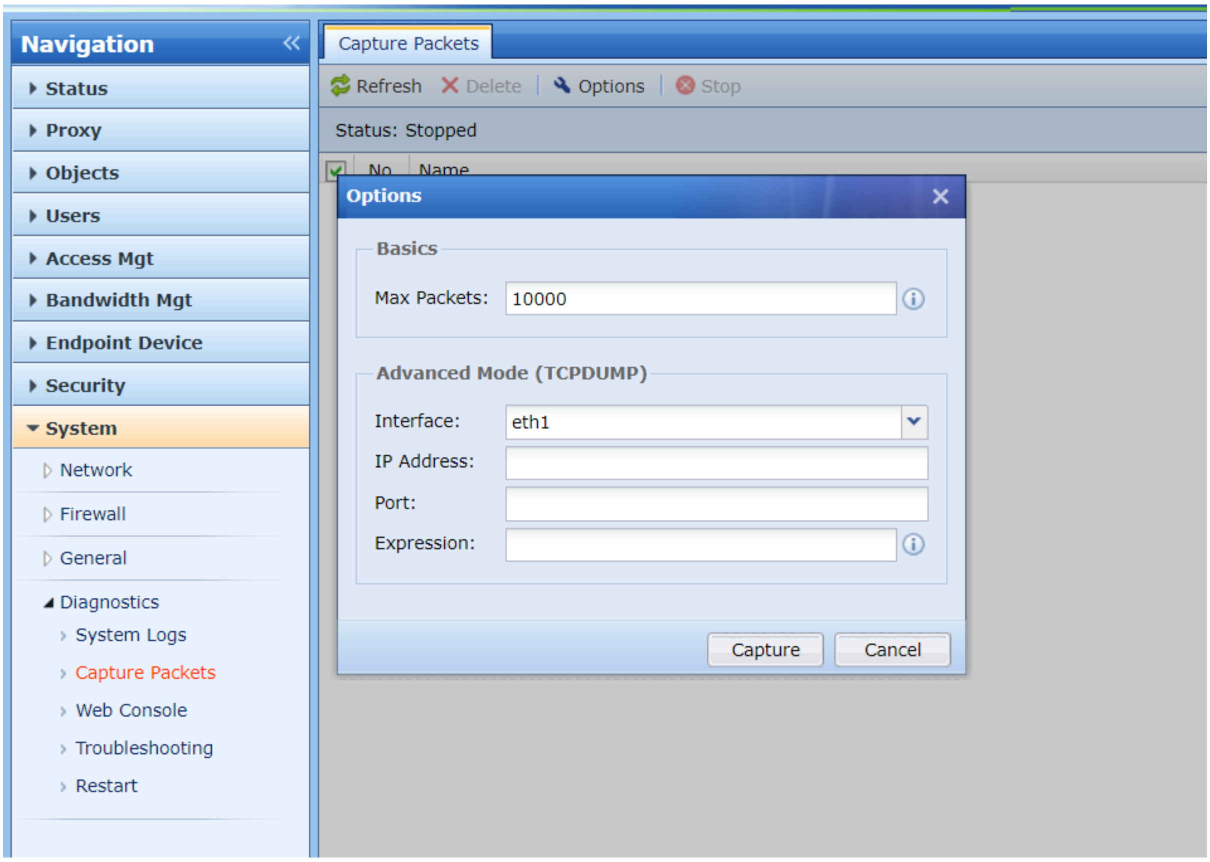
☑ Enable Mirror Interface

Mirror Interfaces (selected interface will be listened):

□	Interface
□	eth0
☑	eth1
□	eth2
□	eth3

2. Configure the switch to mirror the radius traffic to the mirror port of IAM.

3. Capture packets at the mirror port to check whether the data packet is sent to the IAM mirror port.



Status: Stopped

Options

Basics

Max Packets: 10000

Advanced Mode (TCPDUMP)

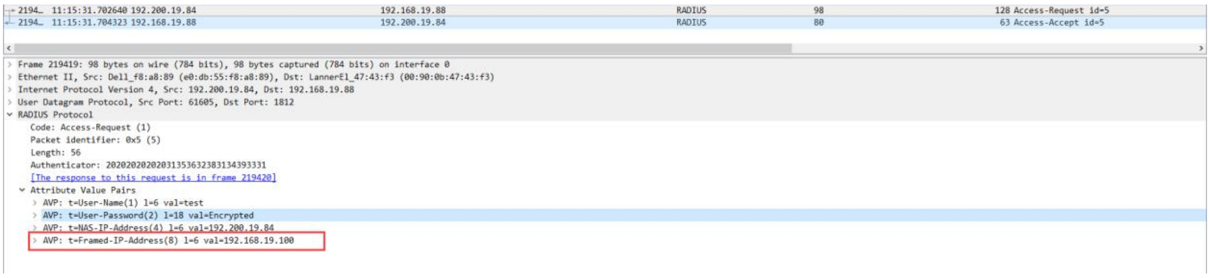
Interface: eth1

IP Address:

Port:

Expression:

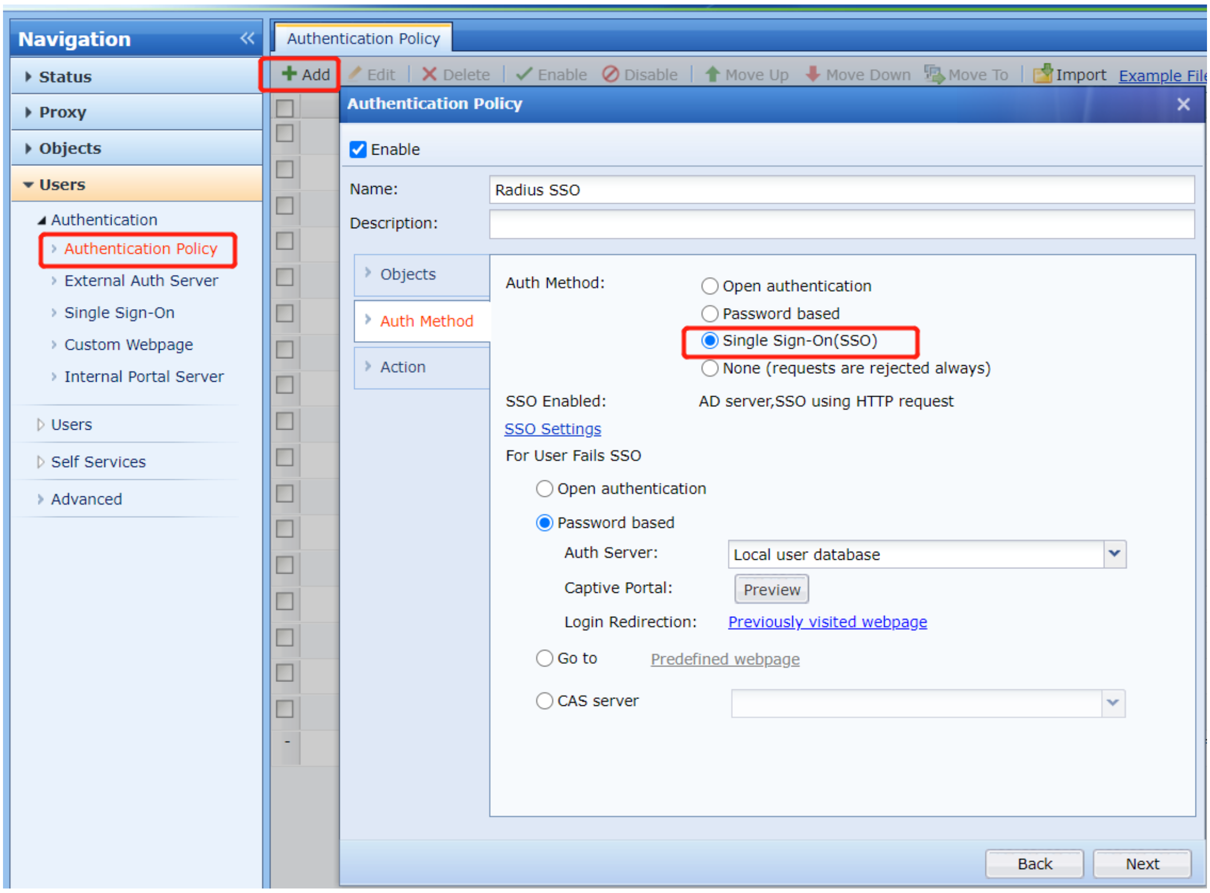
Check whether the packet include the IP address of PC, if packet is not include the PC IP address, IAM will not know which IP will be authenticate. The **NAS-IP-Address** field Record the IP of radius Server, The **Framed-IP-Address** field record the IP of PC. If the user must be authenticated successfully, the packet must include **Framed-IP-Address** and **Username** field. Some packet not contain the **Framed-IP-Address** field, just need configure radius setting in Radius Server.



```
2194… 11:15:31.702640 192.200.19.84     192.168.19.88     RADIUS    98    128 Access-Request id=5
2194… 11:15:31.704323 192.168.19.88     192.200.19.84     RADIUS    80     63 Access-Accept id=5

> Frame 219419: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
> Ethernet II, Src: Dell_f8:a8:89 (e0:db:55:f8:a8:89), Dst: LannerEl_47:43:f3 (00:90:0b:47:43:f3)
> Internet Protocol Version 4, Src: 192.200.19.84, Dst: 192.168.19.88
> User Datagram Protocol, Src Port: 61605, Dst Port: 1812
v RADIUS Protocol
    Code: Access-Request (1)
    Packet identifier: 0x5 (5)
    Length: 56
    Authenticator: 2020202020203135363238313439331
    [The response to this request is in frame 219420]
  v Attribute Value Pairs
    > AVP: t=User-Name(1) l=6 val=test
    > AVP: t=User-Password(2) l=18 val=Encrypted
    > AVP: t=NAS-IP-Address(4) l=6 val=192.200.19.84
    > AVP: t=Framed-IP-Address(8) l=6 val=192.168.19.100
```

4. Create authentication policy and choose SSO.



Authentication Policy

☑ Enable

Name: Radius SSO

Description:

Auth Method:
○ Open authentication
○ Password based
● Single Sign-On(SSO)
○ None (requests are rejected always)

SSO Enabled: AD server,SSO using HTTP request

SSO Settings

For User Fails SSO

○ Open authentication

● Password based

Auth Server: Local user database

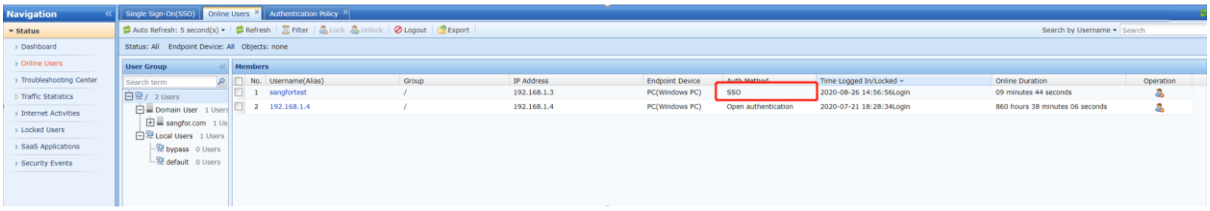
Captive Portal: Preview

Login Redirection: Previously visited webpage

○ Go to Predefined webpage

○ CAS server

5. Then you can see that PC192.168.1.3 is online and the authentication method is SSO on the IAM.



Status: All Endpoint Device: All Objects: none

No.	Username(Alias)	Group	IP Address	Endpoint Device	Auth Method	Time Logged In/Locked	Online Duration	Operation
1	sangfortest	/	192.168.1.3	PC(Windows PC)	SSO	2020-08-26 14:56:56Login	09 minutes 44 seconds	👤
2	192.168.1.4	/	192.168.1.4	PC(Windows PC)	Open authentication	2020-07-21 18:28:34Login	860 hours 38 minutes 06 seconds	👤

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