SANGFOR

IAM

Proxy SSO Configuration Guide

Version 12.0.18

Change Log

Date	Change Description
Dec 12, 2019	Version 12.0.18 document release.

CONTENT

Chapter 1 Function Introduction

Generally applicable to the environment where users use a proxy to surf the Internet, and each user is assigned an account of a proxy server. When using the proxy single sign-on authentication method, when the user passes the authentication of the proxy server, the device also passes the authentication.

1.1 Application Scenarios

Generally applicable to the environment where users use a proxy to surf the Internet, and each user is assigned an account of a proxy server. When using the proxy single sign-on authentication method, when the user passes the authentication of the proxy server, the device also passes the authentication.

1.2 Necessary Description

1. IAM 11.0 device.
2. Lan use proxy to Internet.

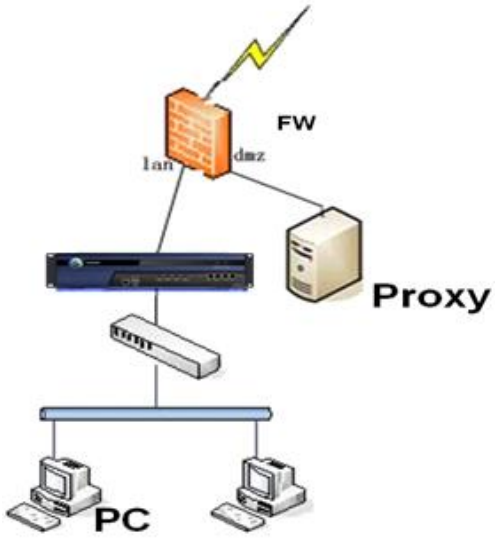
1.3 Configuration Guide

1. Proxy server at Wan direction.
2. Proxy server at Lan direction.
3. Use ISA controller.

1.4 Configuration and Snapshots

1.4.1 Proxy Server at Wan Direction

Proxy single sign-on monitoring mode also completes single sign-on by monitoring login data.
The proxy server is in the direction of the external network, as shown in the figure:



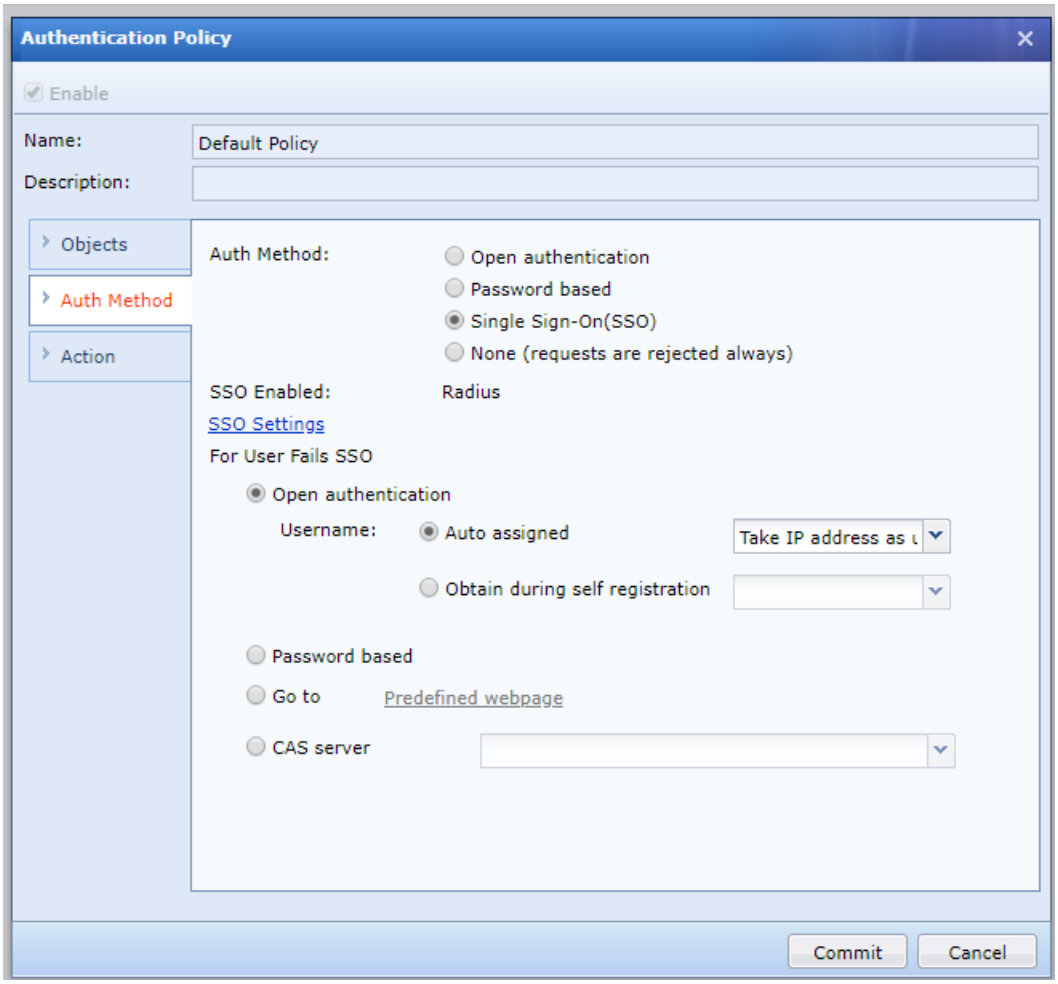
1.4.1.1 Data Flow Process

1. The user goes online through the proxy server, and the device monitors the interaction between the PC and the proxy server
2. The PC is successfully authenticated by the proxy server as well as the device.

1.4.1.2 Configuration Guide

1. Set the Authentication policy

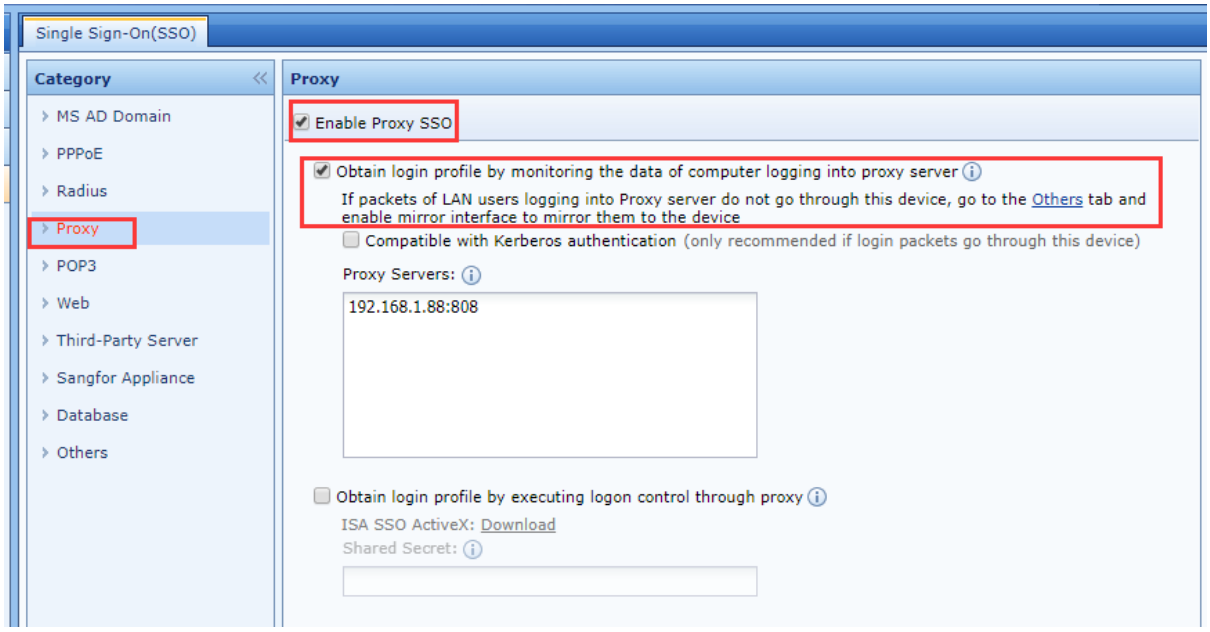
Set the authentication policy for the required SSO user's IP or mac address



2. Configure Proxy SSO

In the [Users] -> [Authentication] -> [Single Sign on] -> [Proxy], check on the [Enable proxy SSO] and click for the [Obtain login profile by monitoring the data of computer logging into proxy server]

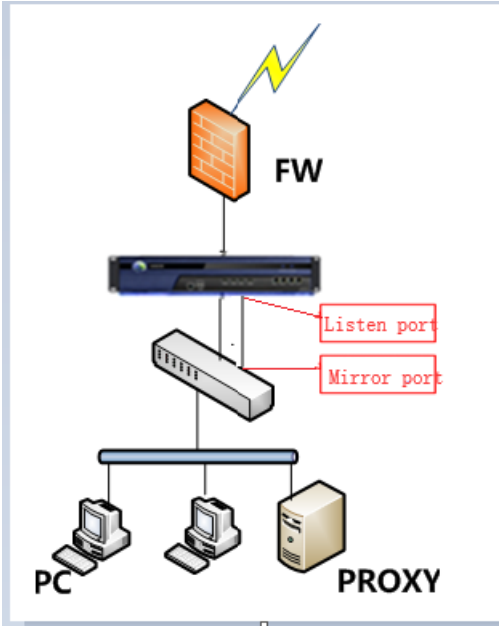
Inside the [Proxy Server], insert the proxy server IP and listening port if has lot of proxy servers, it required add in row by row, here we insert the Proxy server and the listening port.



3. Login test

PC login into the Proxy server, after login success will go online.

1.4.2 Proxy Server at Lan Direction.



1.4.2.1 Data Flow Process

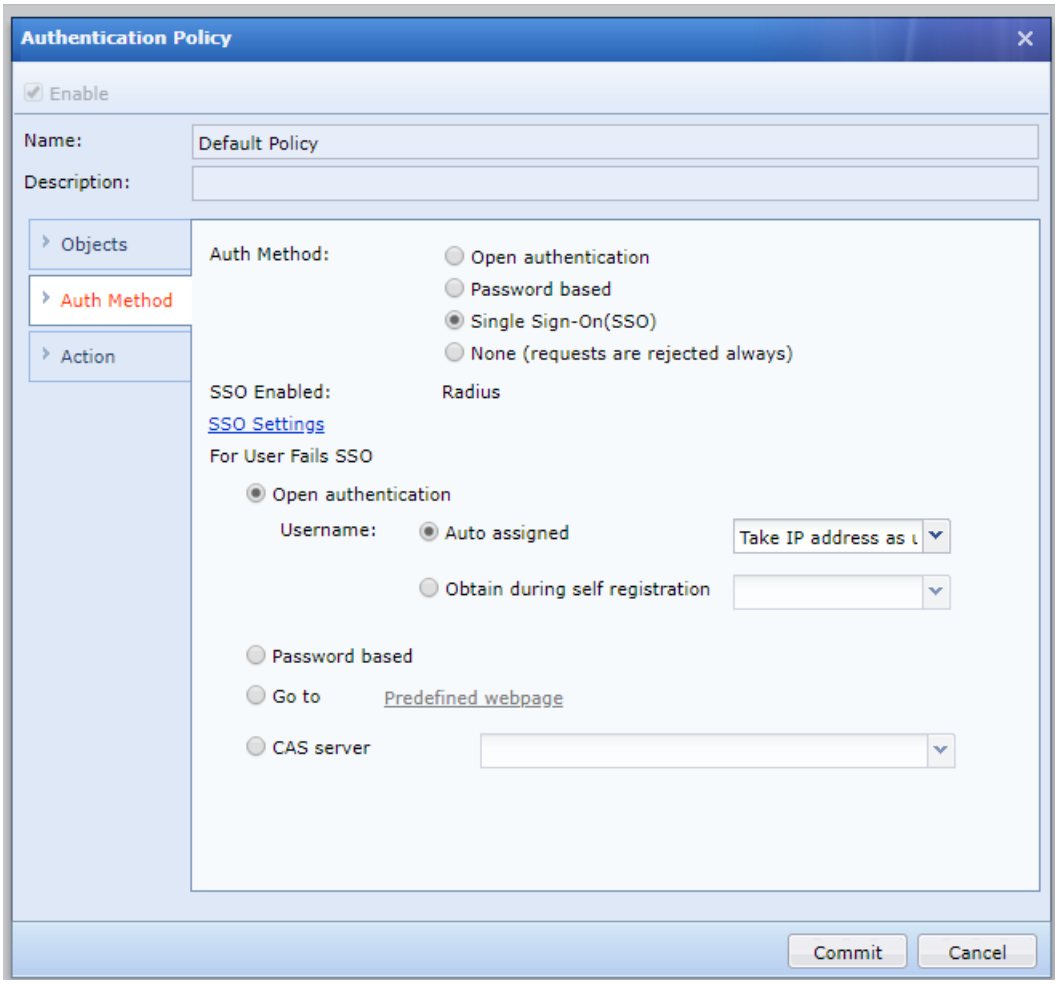
1. The user goes online through the proxy server, and the authentication data is not forwarded by the IAM.
2. Set up a mirror port on the switch to mirror the data from the PC to the proxy server to the IAM
3. The PC is successfully authenticated by the proxy server as well as the device.

1.4.2.2 Configuration Guide

1. Configuration Step

Set the Authentication policy

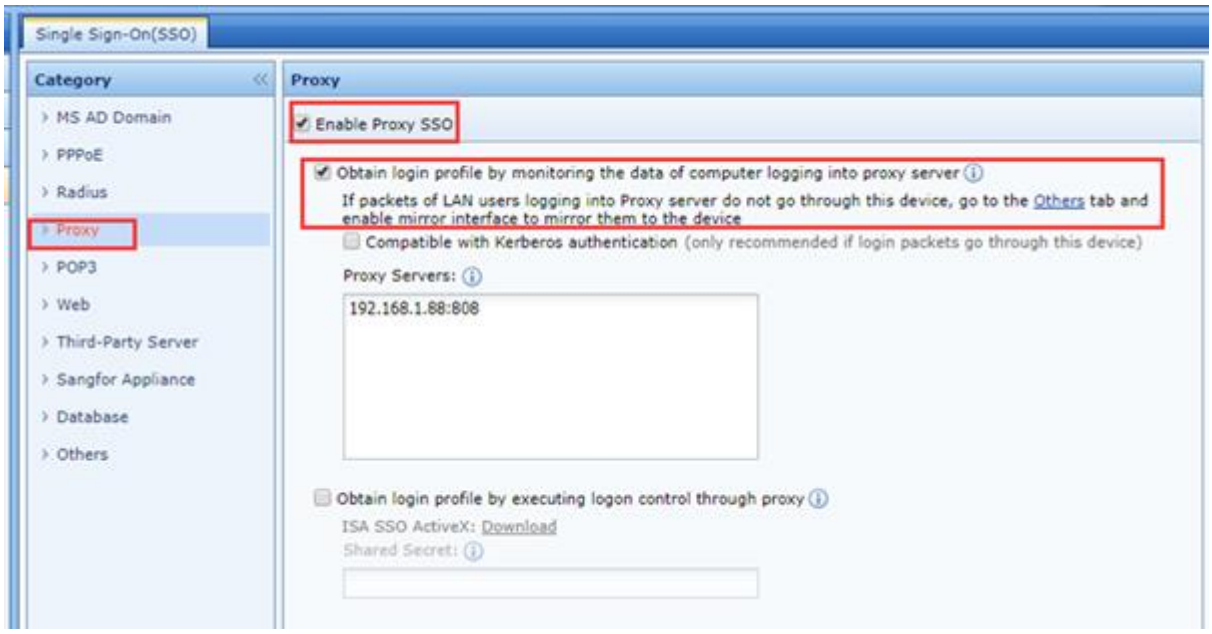
Set the authentication policy for the required SSO user's IP or mac address



2. Configure Proxy SSO

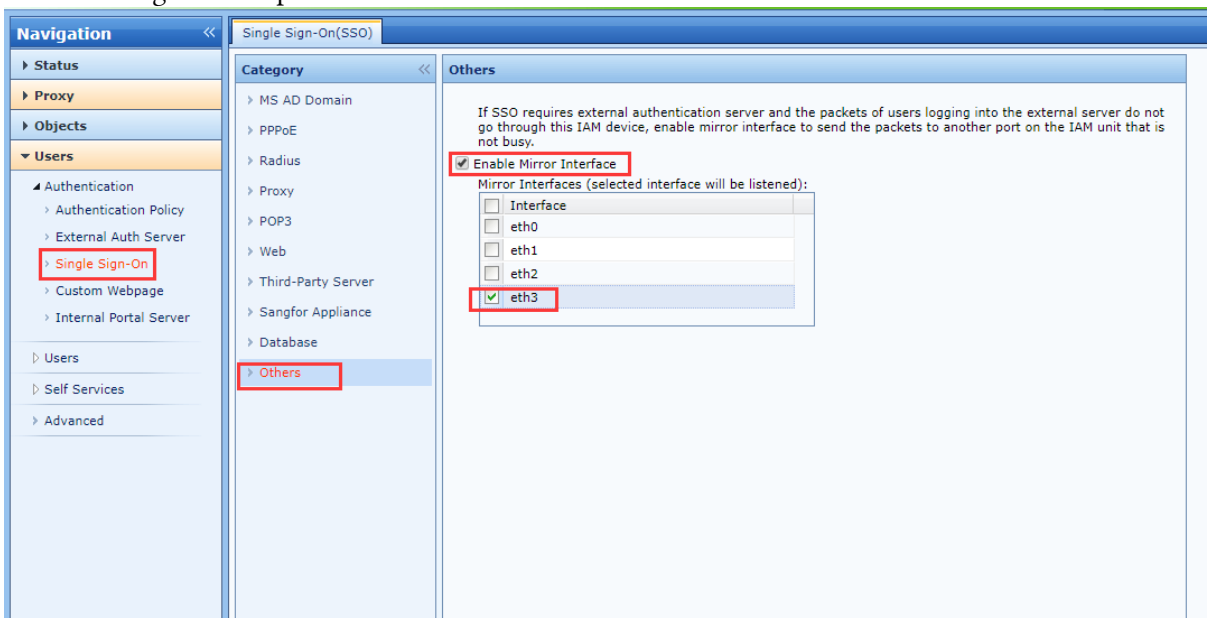
In the [Users] -> [Authentication] -> [Single Sign on] -> [Proxy], check on the [Enable proxy SSO] and click for the [Obtain login profile by monitoring the data of computer logging into proxy server]

Inside the [Proxy Server], insert the proxy server IP and listening port if has lot of proxy servers, it required add in row by row



If the login data does not pass through the device, you need to set the mirror port and connect the mirror

port to the mirror port of the switch that forwards the login data. Click other options to set the mirror port of the device. The mirroring port needs to be set as a free network port. Do not set the network port as a mirroring network port.

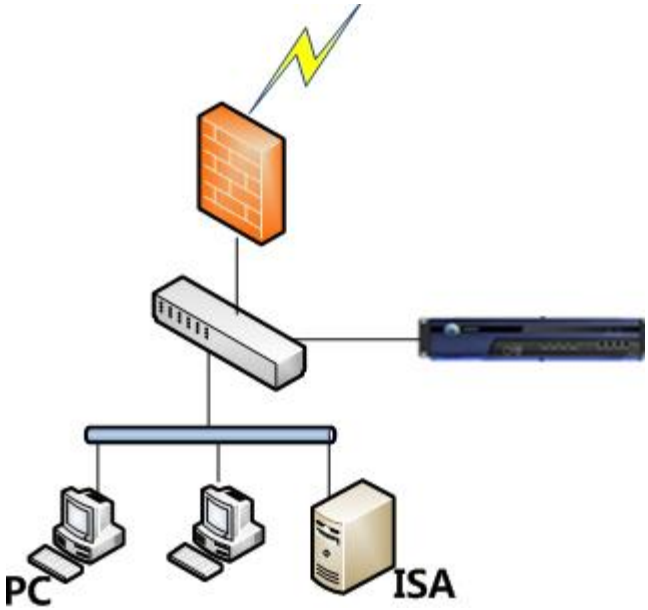


3. Login test

PC login into the Proxy server, after login success will go online.

1.4.3 Use ISA Method

The ISA control method can be used for the ISA server in the internal network. When the data logged in to the ISA does not pass through the device, the extension plug-in is registered on the ISA server, and the information after the PC logs in to the ISA is notified to the device through the extended plug-in. Login on the device. as the picture shows:



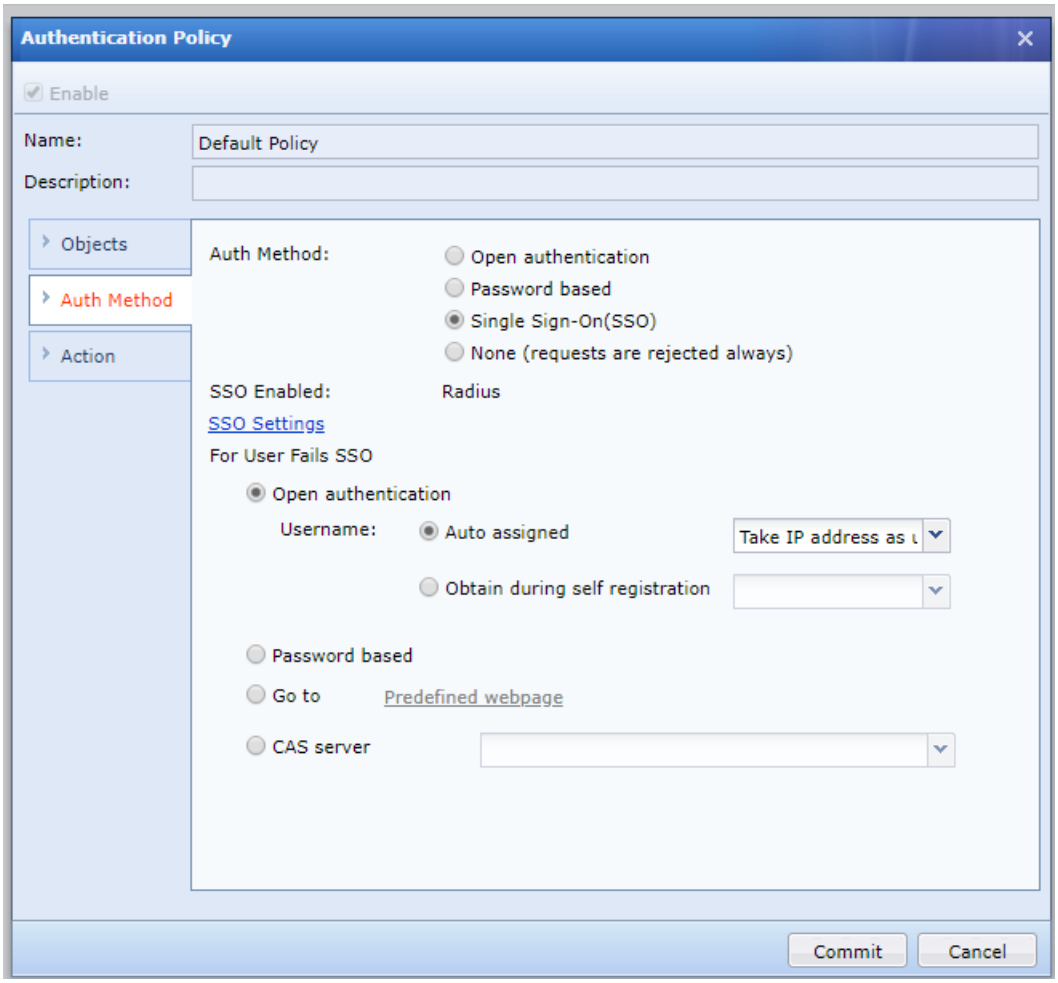
1.4.3.1 Data Flow Process

1. PC passes HTTP proxy and PRXOY authentication of ISA;
2. The ISA sends the information that the PC is successfully logged on to the IAM device;
3. The IAM equipment automatically passes the PC authentication and releases the PC Internet data.

1.4.3.2 Configuration Guide

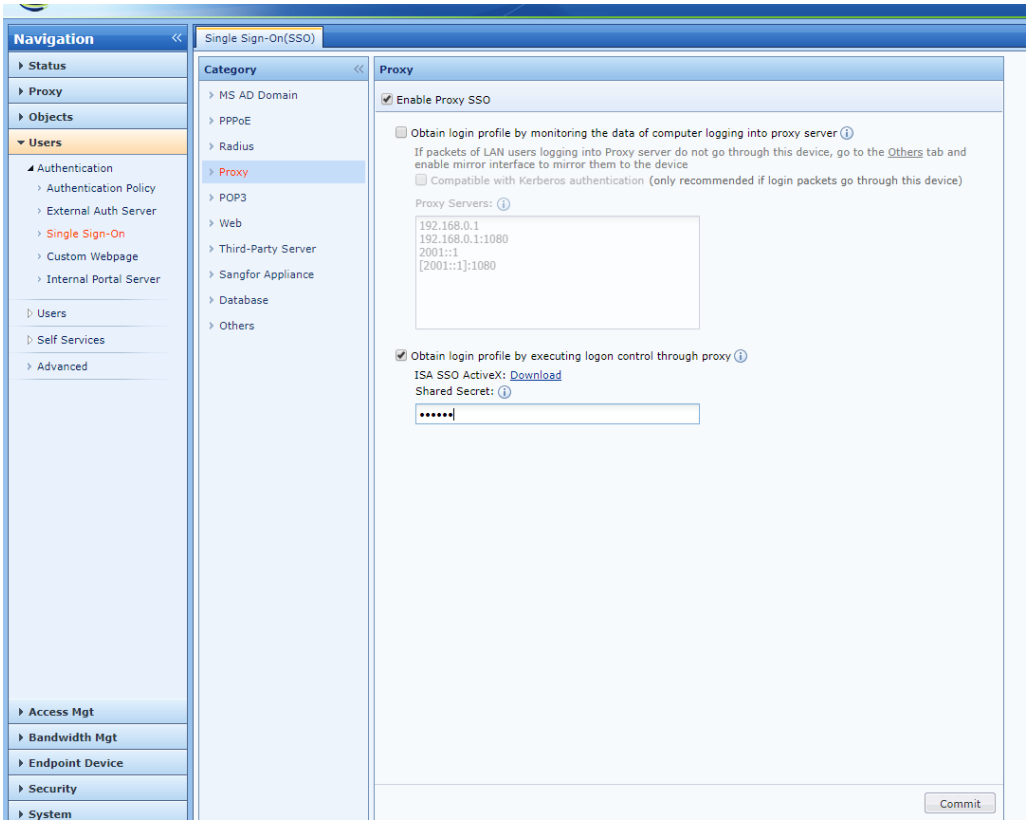
1. Set the Authentication policy

Set the authentication policy for the required SSO user's IP or mac address



2. Configure Proxy SSO

In the [Users] -> [Authentication] -> [Single Sign on] -> [Proxy], check on the [Enable proxy SSO] and click for the [Obtain login profile by executing logon control through proxy] and insert the shared key.



1.4.3.3 ISA Single Sign-on Control Configuration

Download the ISA single sign-on control and example on the device, configure the ISA server, register the plug-in, and configure SangforAC.ini.

1. The plugin MyAuthFilter.dll is placed in the ISA installation directory, such as C: \ Program Files \ ISA Server \

2. Run the regsvr32 "C: \ Program Files \ ISA Server \ MyAuthFilter.dll" XML plugin

3. Put the sample configuration file SangforAC.ini in the root directory of drive C.

[Configuration]

IAMip = 192.168.0.1 device IP address

key = 123 The data packet encryption key for logging in to ISA, which must be the same as that set on the device

cycle = 30 The minimum interval (unit: second) for each IP address to send login data packets. The purpose is to prevent each IP address from sending a login data packet every time a new session is accessed to a new website.

logpath = debug log path. If it is empty, it means that the log is turned off. If it is filled, it means that the log is turned on. Set it to be off. Please turn it on when necessary.

maxlogsize = 1 The maximum size of the debug log file (unit: MB). When the log file reaches the previous level, it will be automatically emptied.

charset = UTF-8 supports UTF-8, UTF-16, GB2312, GB18030, BIG5

Confirm that the "Sangfor ISA Auth Filter" plugin is enabled in the ISA plugin panel.

Login test

PC login into the Proxy server, after login success will go online.

Chapter 2 Precaution

2.1 Proxy Server at WAN Direction

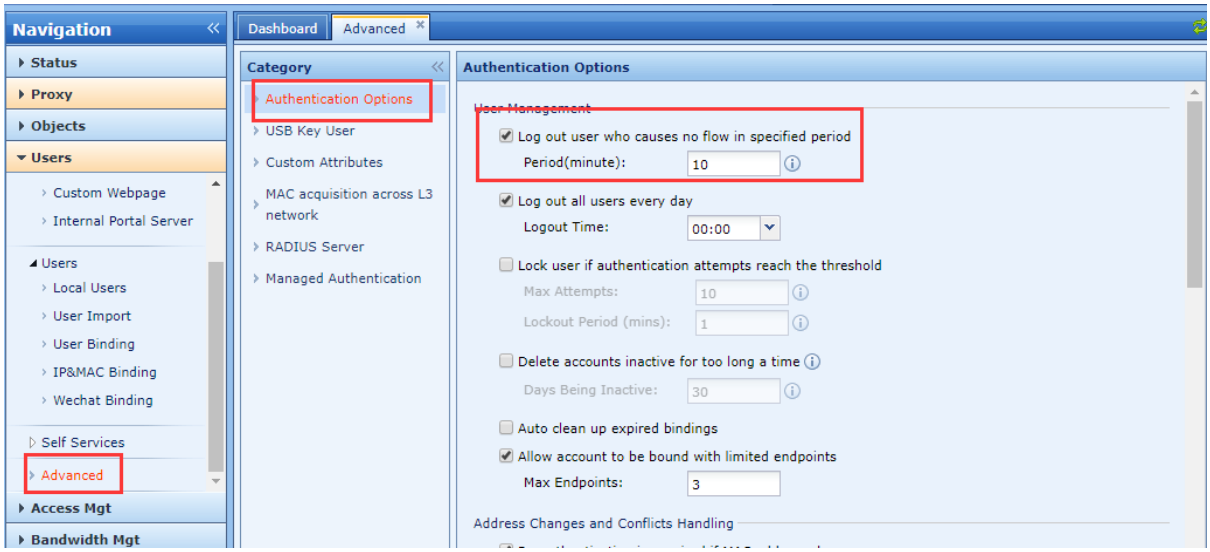
1. If the proxy server is an ISA server and the ISA server uses the "windows integrated identity authentication" method, you need to check [Compatible with kerberos authentication method] to complete single sign-on, and this method is only applicable to login packets passing through the AC device In this case, it is not applicable to mirror mode, and it is not supported in bypass mode.
2. In this scenario, if [Show Disclaimer] is selected in [Authentication Policy] → [Post-Authentication Processing] → [Advanced Options], you need to configure redirection from the DMZ port, otherwise you will not be able to access the Internet through authentication.

2.2 Proxy Server at LAN Direction

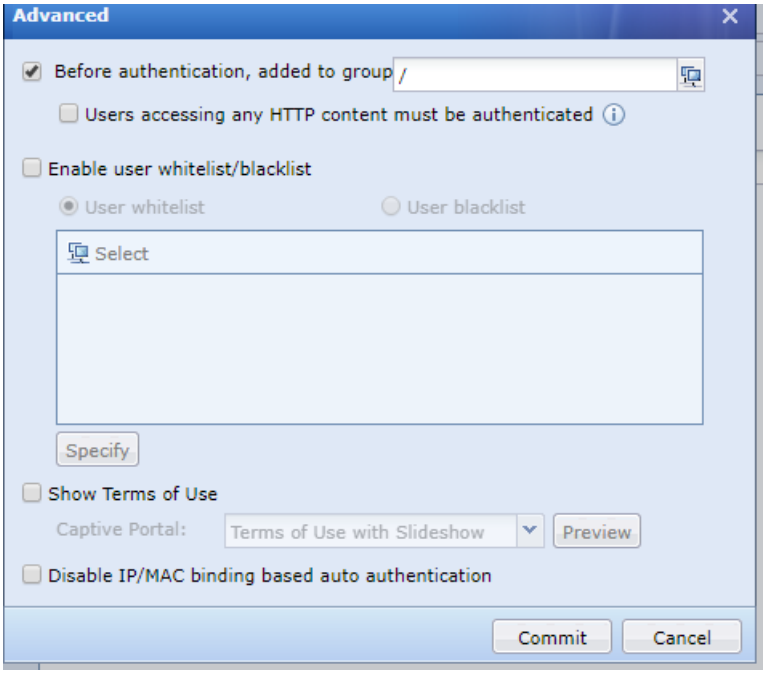
This type of login data does not pass AC, and the monitoring method using mirrored data does not support [compatible Kerberos authentication method]

2.3 Using the ISA Control Method

1. Every time you modify the SangforAC.ini file, you need to re-register the plugin
2. The ISA plug-in cannot enable the domain user to automatically log off the device when the domain user logs off or shuts down the computer. However, you can set the timeout period on the device console to let users automatically log off from the device. As shown below:



3. The IAM and ISA server keys must be the same, and this key must not be the same as the other single sign-on keys.
4. The ISA server must release the data connected to the UDP port 1773 of the IAM device.
5. If the proxy server is in the IAM WAN area, you need to grant access to the proxy server before user authentication.
6. How to grant permissions?
7. In [Authentication Policy]-[Action]-[Advanced], check [Before authentication, added to group] and set a group.



Pass the IP and port of the proxy server in this user group's Internet permission settings.

SANGFOR