# How to Configure AD SSO Scripts

### I Overview

This document presents how SANGFOR SSO logon script program is configured on Active Directory (AD) domain to have the users log in to the SANGFOR IAM gateway device once they have logged in to the AD domain.

### **II Basic Setups**

### Configure Logon Script Program

**Step 1.** Log into the AD server. Click [Manage Your Server] and then [Manage users and computers Active Directory] to enter the [Active Directory User and Computers] page, as shown below:



**Step 2.** Right-click the domain to be monitored and click [Properties] to enter the [Properties] page. Click the [Group Policy] tab, as shown below:

My Documents	drive	
<b>3</b>	Sective Directory Users and Compu	iters
My Computer	Eile Action View Window He	pX
		8 🔁 🚾 💩 🗸 🍕 📶
	Active Directory Users and Computer	yuanbo.163.com 5 objects
	E Saved Queries	Name Type Description
My Network		Builtin builtinDomain
FIGUES		Computers Container Default container for upgr
-		Expreint Container Default container for seru
<b>9</b>		Users Container Default container for upgr
Recycle Bin		yuanbo.163.com Properties
		General Managed Bu Group Policy
<b>&gt;</b>		To improve Group Policy management upgrade to the Group Policy Management Console (GPMC)
Internet Explorer		
		Current Group Policy Object Links for yuanbo
<u>k</u>		
		Group Policy Object Links No Override Disabled
Adobe Reader 8		Default Domain Policy
2		
Sacurity		
Configurati		
		This list obtained from: viw-ov7z5bu123d.vuanbo.163.com
<u></u>		
AdheRdr81		
		Options         Delete         Properties         Down
-		
		Block Policy inheritance
SSO.pdf		
		OK Cancel Apply

**Step 3.** Double-click the object "Default Domain Policy" and edit the logon/logoff script on the pop-up page [Group Policy Object Editor].

Elle     Action     View     Help       Image: Second S	
← →       •	
Software Settings     Logon       Image: Computer Configuration     Image: Computer Settings	
<ul> <li>Bescription: Contains user logon scripts.</li> <li>Windows Settings</li> <li>Folder Redirection</li> <li>Folder Redirection</li> <li>Administrative Templates</li> </ul>	on/Logoff)
Extended Standard	lard /

Step 4. Double-click "Logon" script to enter the pop-up [Logon Properties] dialog; click the

<Show File> button and add the logon.exe file into the scripts list.

Group Policy Object Editor		<u>_0×</u>
Image: Section	Logon Properties Scripts Logon Scripts for Default Domain Policy	2 X
Administrative Templates	To view the script files stored in this Group Policy Object, press the button below. Show Files OK Cancel	edit emove Apply

2	\\yuanbo.163.com\sysvol\y	uanbo.163.com\P	olicies\{31B2F3	340-016D-11D2-945F-00C0	)4FB984F9}\User\Scr	
1000	Eile Edit View Favorites I	ools <u>H</u> elp				27
8	3) Back 🔹 🕤 👻 🧊 🔎 Searc	:h 🜔 Folders 📗	\$ 3 × 9			
1	Address 🛅 \\yuanbo.163.com\sysvol\yuanbo.163.com\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\User\Scripts\Logon					
	lame 🔺	Size	Туре	Date Modified	Attributes	
	logon.exe	0 KB	Application	10/29/2008 7:09 PM	A	

**Step 5.** Under the [Logon Properties] page, click the <Add> button to enter the [Add a Script] dialog. Type in the script parameters; the value of [Script Parameters] consists of three sections: the first section is the IP address of LAN interface that is accessible for the LAN users; the second section is the listening port number (1775, unchangeable); the third section is the communication key (it must be the same as the key configured on the [Authentication Option] > [AD Domain] tab, as shown below). Finally, click the <OK> button and then the <Apply> button to complete configuring the logon script. This script will automatically run when the domain user logs in.

	Add a Script		<u>? ×</u>	
	Script <u>N</u> ame:			
	logon.exe		Browse	
	Script <u>P</u> aram			
	10.251.251.	254 I//b 123		
		OK	Cancel	
Sign NGAF Platform (80.35)	Home SOC	Monitor Policies Objects Network System	Menu name	Q
Policies =	< 212 >	Note: The incense is not activated, which will impact device teature and Note: The incense is not activated, which will impact device teature and Note: The incense is not activated, which will impact device teature and Note: The incense is not activated, which will impact device teature and Note: The incense is not activated, which will impact device teature and Note: The incense is not activated, which will impact device teature and Note: The incense is not activated, which will impact device teature and Note: The incense is not activated, which will impact device teature and Note: The incense is not activated, which will impact device teature and Note: The incense is not activated, which will impact device teature and Note: The incense is not activated activate	valiabulity. Please activate the license as soon as possible. Licensing	
) Access Control >	Authentication Options			
	Options <i< td=""><td>SSO Options</td><td></td><td></td></i<>	SSO Options		
inetwork security	SSO Options	Client-Side Domain SSO Proxy SSO POP3 SSO Web SSO RADIUS Oth	ers	
E Decryption	Auth Page Redirection	Enable Client-Side Domain SSO     Obtain testin profile two constitutes testin profile through demain		
③ Bandwidth Management >	Authentication Conflict	Download Domain SSO Program		
Authentication ~	Others	Shared Key (): 🚥 🐱		
Local Users	Others	Domain SSO     Denviron SSO     Denver for user contentials		
Group/User     Iser Import		Add   1 1 Delete		
LDAP User Sync		Domain Controller Domain Name Last Obtained Recent Users Status	· • •	
<ul> <li>User Authentication</li> </ul>				
Authentication Policy				
Authentication Options	No data available			
<ul> <li>External Auth Server</li> </ul>				
Custom Webpage	Save			

## Configure Logoff Script Program

**Step 6.** Under the [Group Policy Object Editor] page (please go back to Step 3 and conduct the similar operations), double-click the "Logoff" script to enter the [Add a Script] dialog. Type in the script parameters (IP address of the SANGFOR IAM gateway device). Finally, click the <OK> button and then the <Apply> button to complete configuring the logoff script program. The domain user will automatically log out of the IAM device when it logs off or the computer turns off.

Browse

### **III** Advanced Setups

If the above basic setups do not meet your needs for some other situations (take the following two cases for example), you can follow the steps below to set the advanced options.

- a.) The local area network (LAN) is divided into several VLAN network segments; the IAM gateway device is configured with multiple VLAN addresses. In this situation, the IP addresses accessible for the LAN users of different VLANs are not the same. However, the basic setup only allows you to configure one IP address, which is unable to meet the requirement.
- b.) The network has multiple AD domains and each domain is allocated with an IAM device, but the configurations will be automatically synchronized among the domains, including the group policy. Therefore, domain of a different IAM device cannot be configured with a distinguishable SSO logon script of its own.

#### **Setup Steps**

**Step 1.** Open the configuration file "sinforIP" (in the SSO Script Program compressed package) with notepad, edit the file by following the instructions as shown in the following figures. It works like this: the program reads this configuration file, and searches for the IP address of the corresponding device according to the DNS settings (generally, it is the same as the domain server IP) of the current user and then send the SSO logon packet to the IP address. If multiple matching IP addresses have been searched, the program will send the SSO logon data packet to each device IP address.

```
[config]
count = 3
                                  Domain server IP, which is commonly the DNS address
[0]
                                  configured on the user PC
depict = VLAN-5(R&D Dept)
domainIP = <u>192.168.8.6</u>
sangforIP = 192.168.5.2
                                 Device IP
shareKey = 123
                               Shared key for
                               communication
[1]
depict = VLAN-5(Marketing Dept)
domainIP = 192.168.8.6
sangforIP = 192.168.2.2
shareKey = 321
[2]
depict = VLAN-5(Headquarters)
domainIP = 192.168.8.6
sangforIP = 192.168.7.2
shareKey = 123
```

```
[config]
count = 3
[0]
depict = Haikou Headquarters
domainIP = 192.168.21.25
                                         For the second case above, the settings of
sangforIP = 192.168.21.5
                                         domain servers and devices at different sites
shareKey = 123
                                         can be different, but the settings of group
                                         policies should be the same.
[1]
depict = Beijing Operation Dept
domainIP = 10.172.5.2
sangforIP = 10.172.5.8
shareKey = 321
[2]
depict = Shenzhen Logistics Dept
domainIP = 10.172.8.64
sangforIP = 10.172.8.9
shareKey = 123
```

**Step 2.** Having modified the configuration file "sinforIP", you need make a copy of it and paste it into the directory where the logon.exe file locates (please refer to the Step 4 of Basic Setups). Please note that you need not enter the script parameter this time, as shown below:

Add a Script	<u>?×</u>
Script <u>N</u> ame:	
logff_release.exe	Browse
Script Parameters:	
ОК	Cancel
need not enter the script parameter	

**Step 3.** Operations are similar to that of Step 2. Make a copy of "sinforIP" and paste it into the directory where the logff.exe file locates. Please note that you need not enter the script parameter this time.