How to Configure AD SSO Scripts

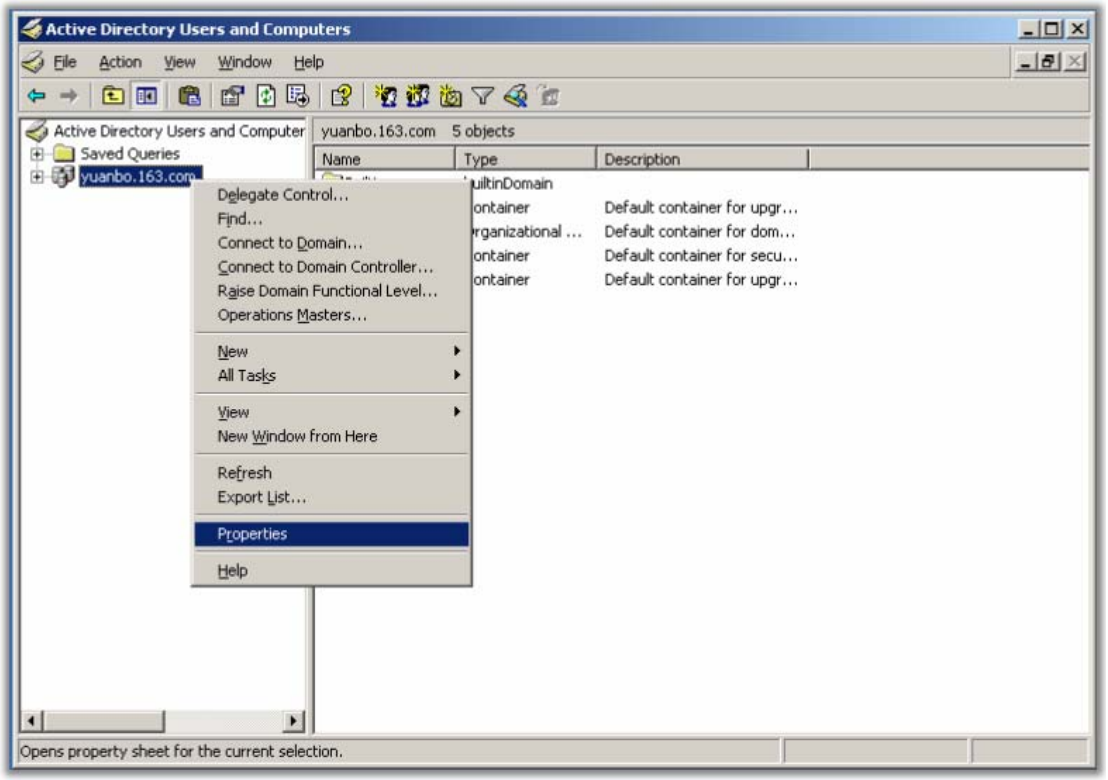
Ⅰ Overview

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.

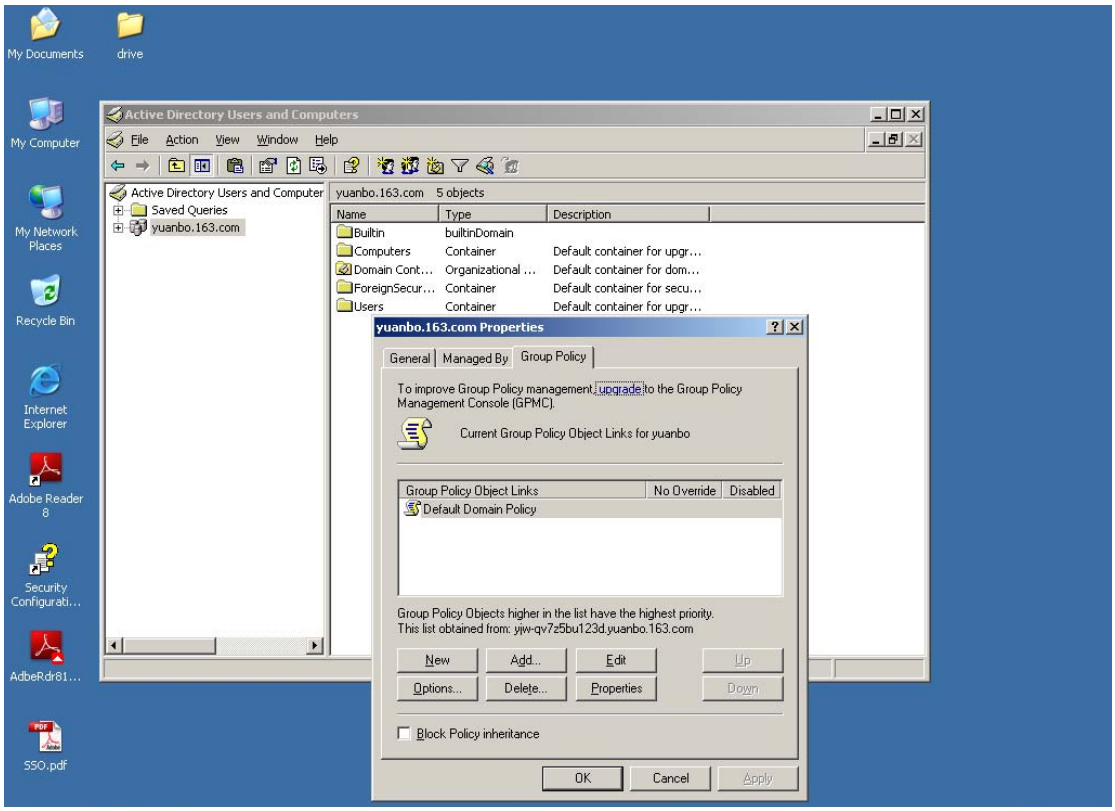
Ⅱ Basic Setups

➢ Configure Logon Script Program

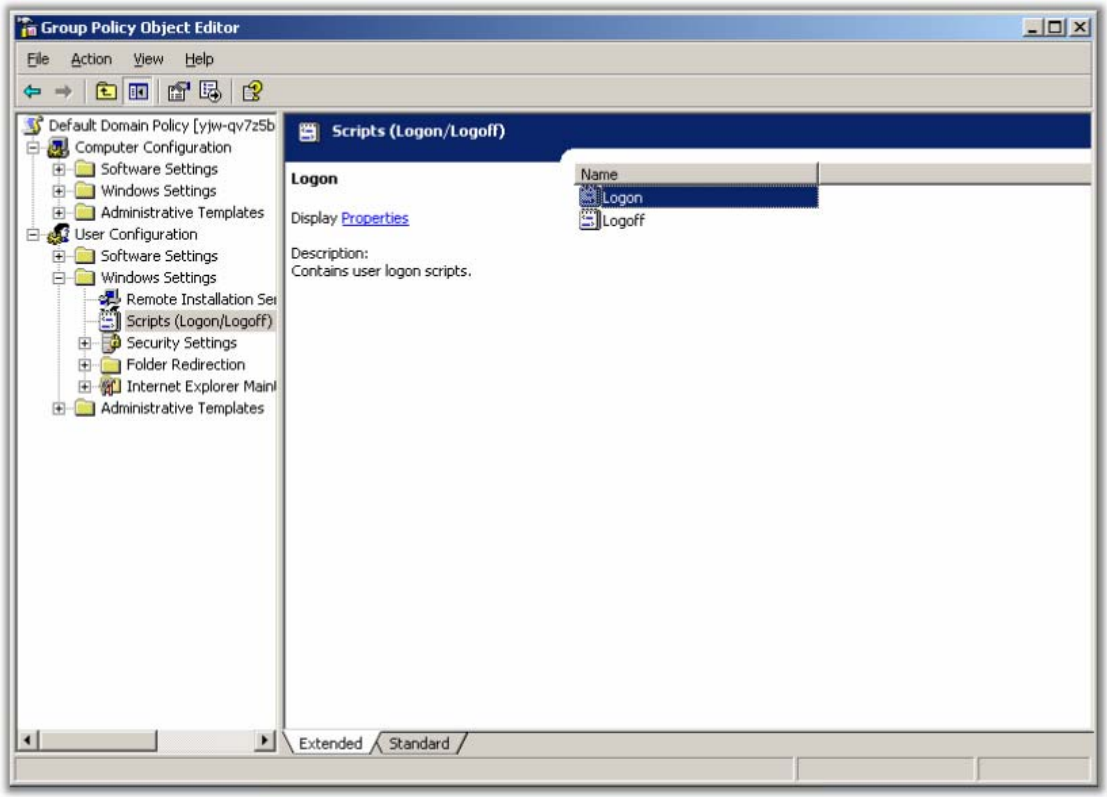
Step 1. Log into the AD server. Click [Manage Your Server] and then [Manage users and computers Active Directory] to enter the [Active Directory User and Computers] page, as shown below:



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:

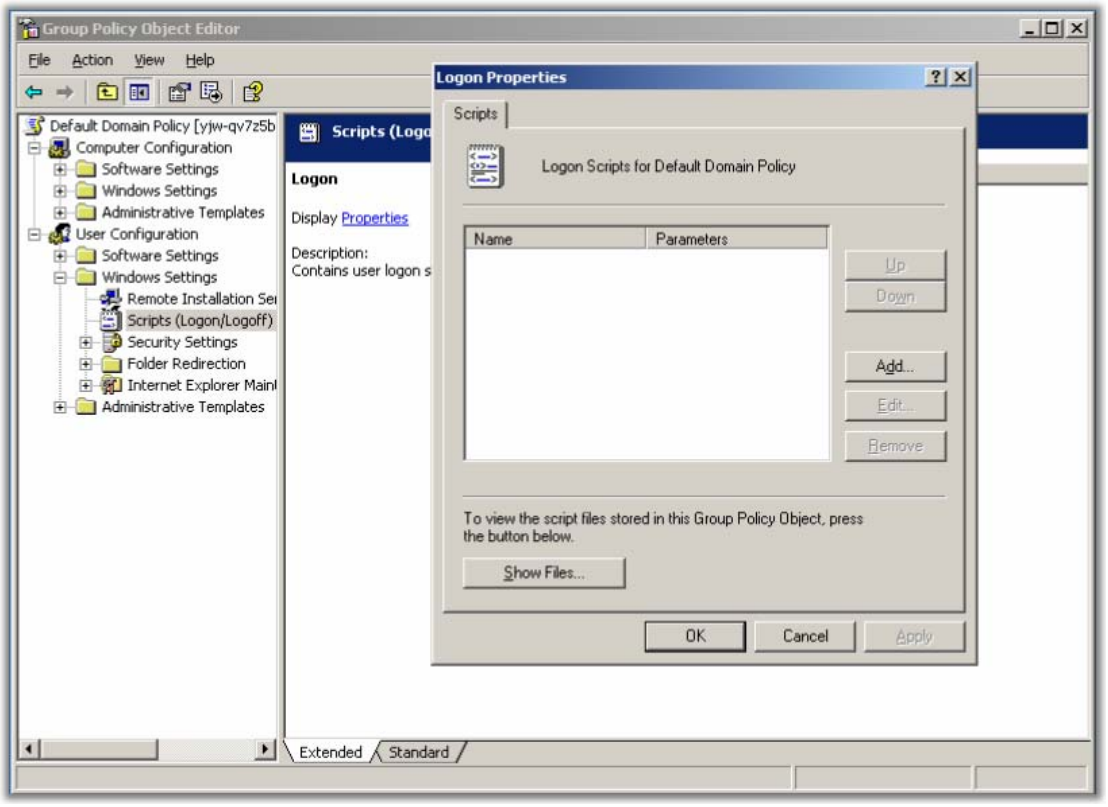


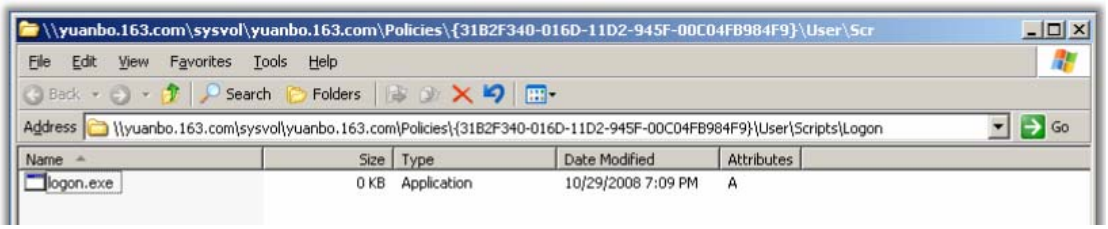
Step 3. Double-click the object “Default Domain Policy” and edit the logon/logoff script on the pop-up page [Group Policy Object Editor].



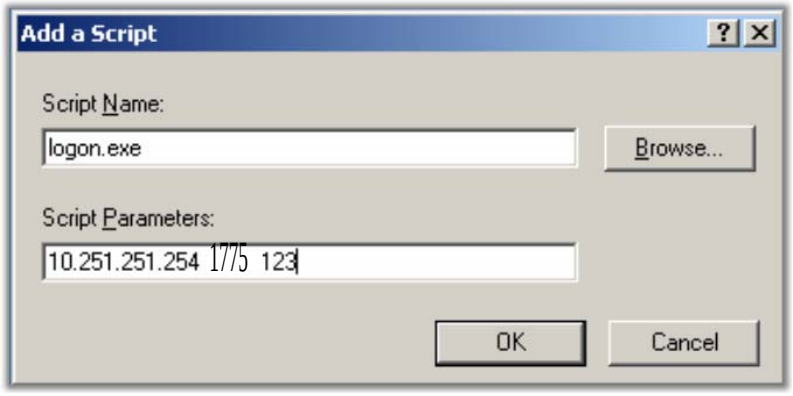
Step 4. Double-click “Logon” script to enter the pop-up [Logon Properties] dialog; click the

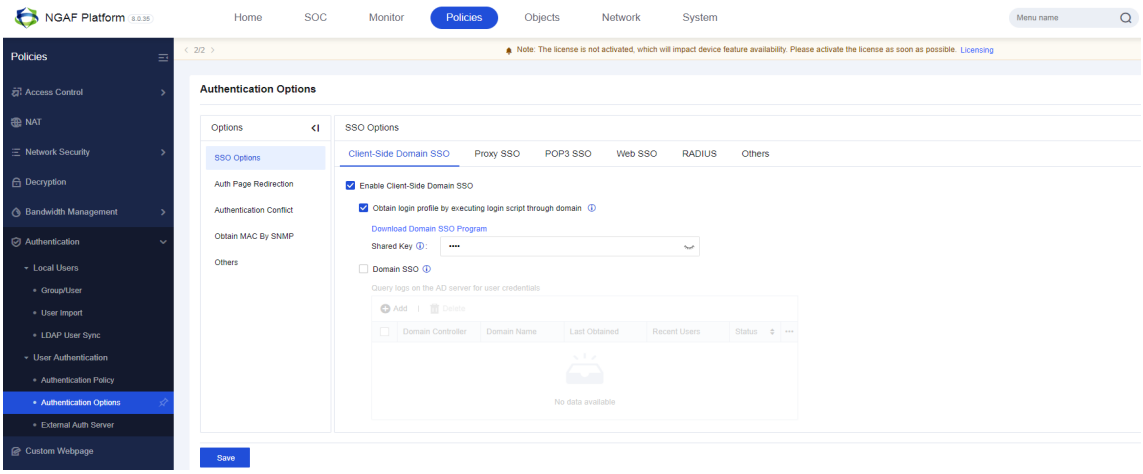
<Show File> button and add the logon.exe file into the scripts list.





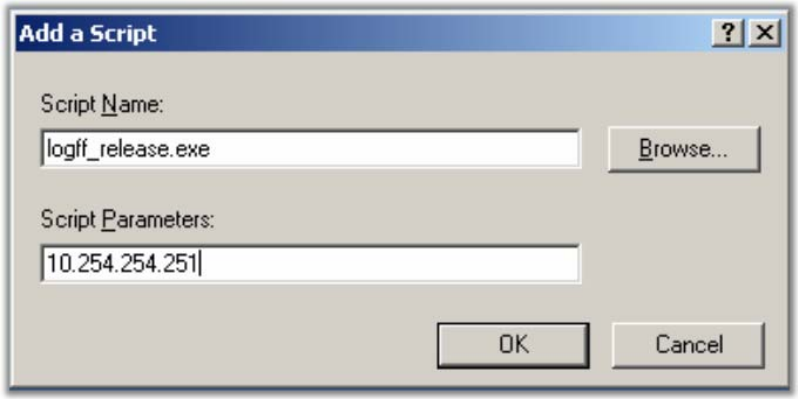
Step 5. Under the [Logon Properties] page, click the <Add> button to enter the [Add a Script] dialog. Type in the script parameters; the value of [Script Parameters] consists of three sections: the first section is the IP address of LAN interface that is accessible for the LAN users; the second section 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.





➢ 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.



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

[0]
depict = VLAN-5(R&D Dept)
domainIP = 192.168.8.6
sangforIP = 192.168.5.2
shareKey = 123

[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
```

Domain server IP, which is commonly the DNS address configured on the user PC

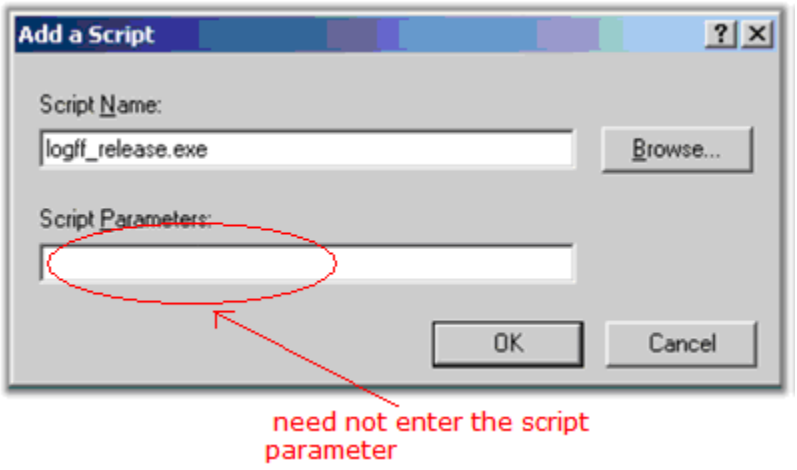
Device IP

Shared key for communication

```
[config]
count = 3

[0]
depict = Haikou Headquarters
domainIP = 192.168.21.25
sangforIP = 192.168.21.5
shareKey = 123

[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
```

For the second case above, the settings of domain servers and devices at different sites can be different, but the settings of group policies should be the same.

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:



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.