SANGFOR

IAM

Script SSO Troubleshooting Guide

Version 12.0.18

Change Log

Date	Change Description
Dec 2, 2019	Version 12.0.18 document release.

CONTENT

Chapter 1 Troubleshooting 1
1 The PC requests to join the domain 1
2 Data interaction after PC joins the domain 2
3 PC runs logon.exe 6
Chapter 2 Common issue 9
2.1 Users intermittently go online and offline on IAM 9
2.2 Domain users go online in IAM but cannot access the Internet 10
2.3 Domain users are not online on IAM but the logon process is running on the PC 10
2.4 Domain users are not online on IAM and no logon process is running on the PC 11
Chapter 3 Precautions 12

Chapter 1 Troubleshooting

Summary of troubleshooting methods

Analysis from the data interaction process of the authentication process

1. The PC requests to join the domain

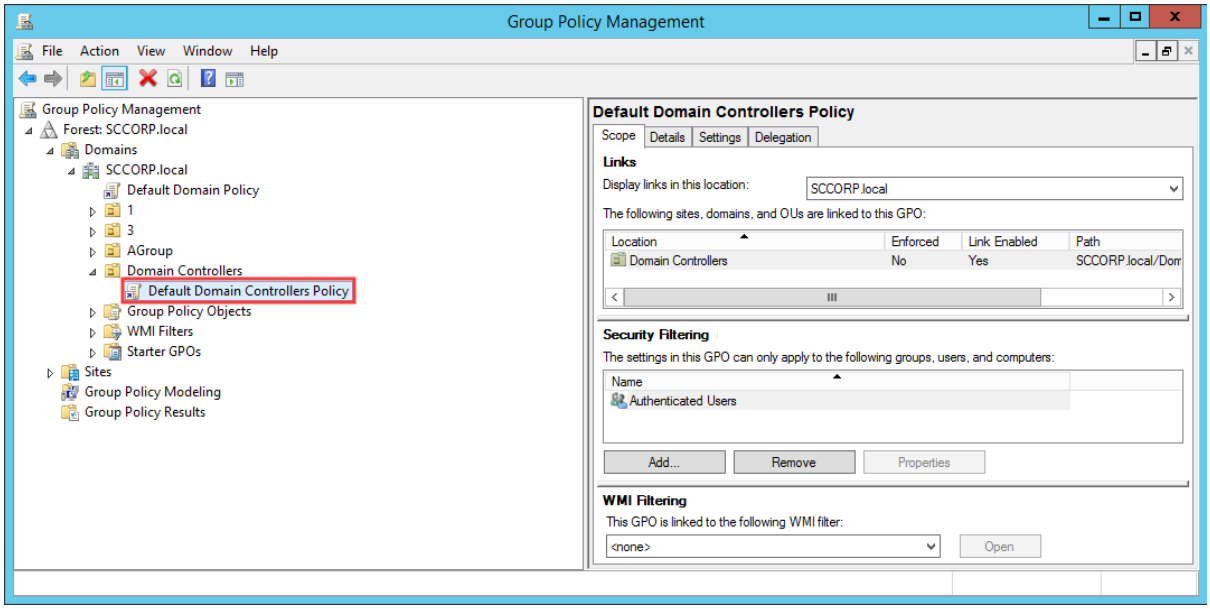
2. Successfully joined the domain data exchange after domain authentication successful.

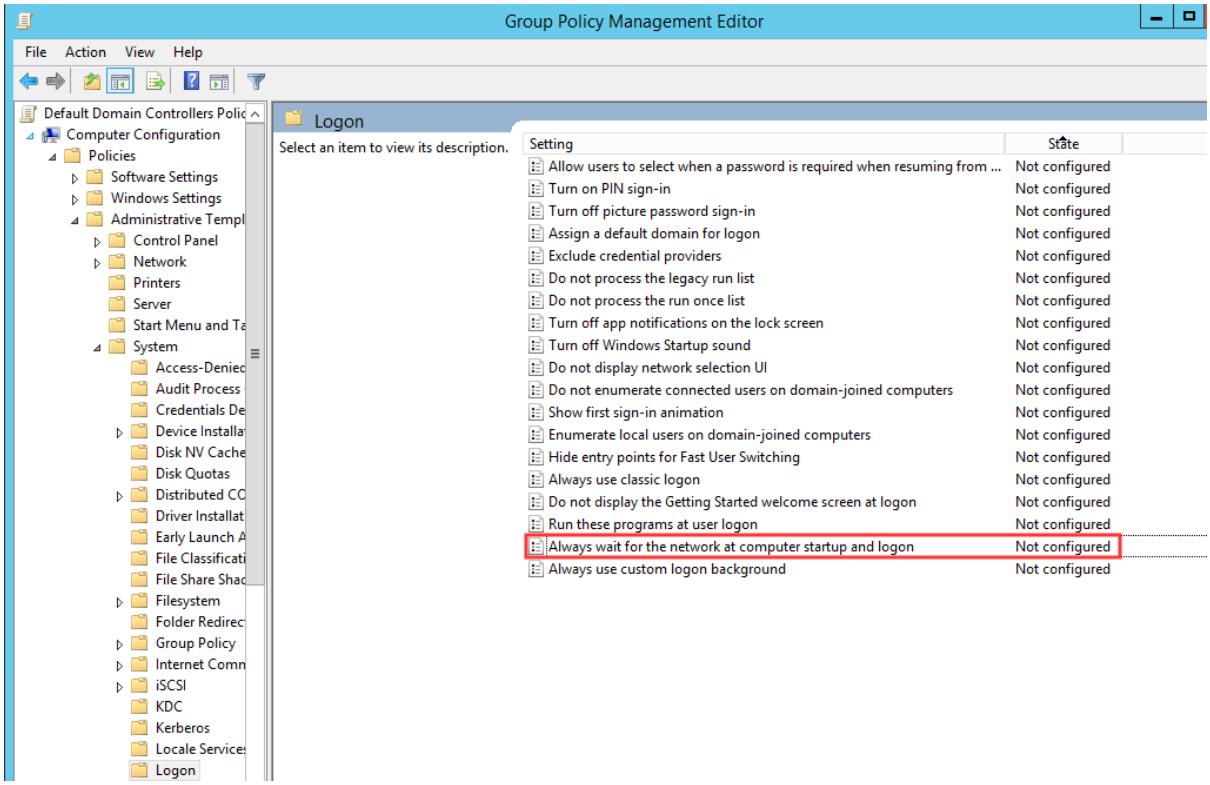
3. PC runs logon.exe

1 The PC requests to join the domain

When using scripted SSO, the PC itself needs to join the AD domain first, and usually no problem occurs. However, if the PC joins the AD domain offline or the PC has a connection to the public network before joining the AD domain, single sign-on may fail.

In this case, it is recommended to enable the domain group policy "Always wait for network when computer starts or logs on." Use the command "gpupdate.exe / force" on the AD domain server to update the group policy.





2 Data interaction after PC joins the domain

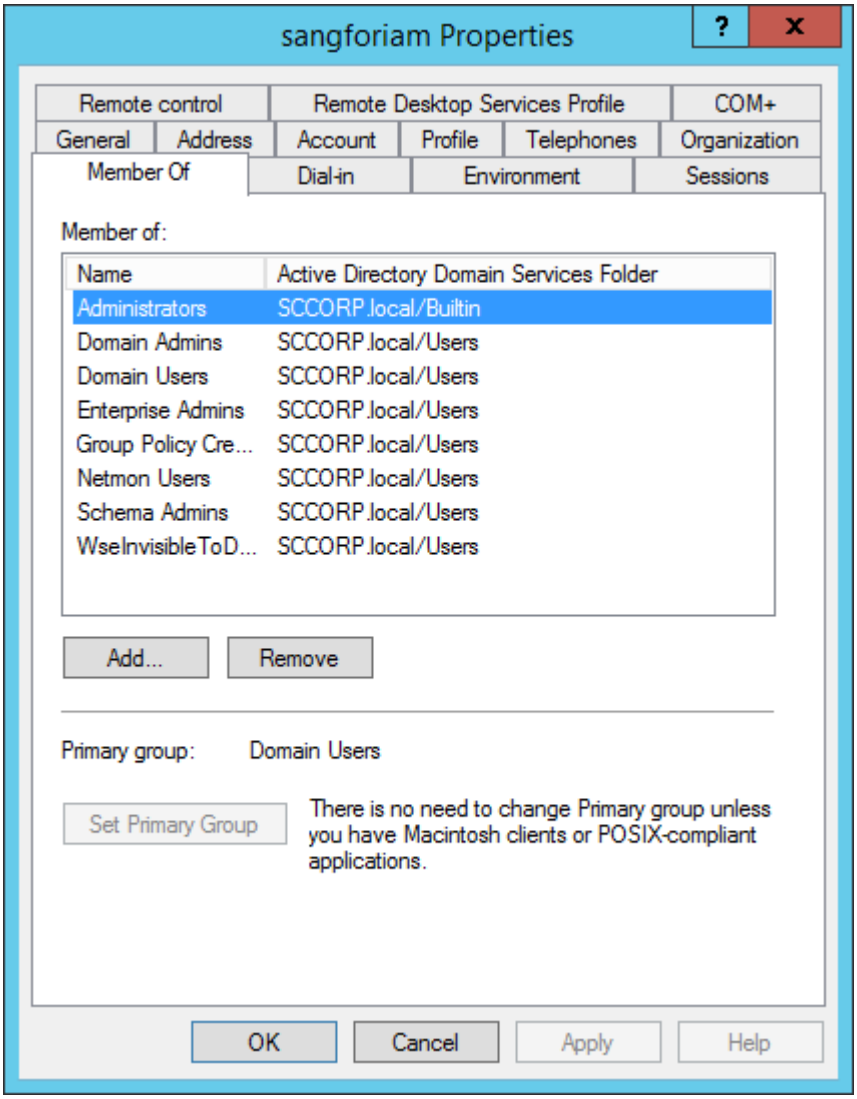
After the PC successfully joins the AD domain, the logon.exe script is executed. The following factors can cause domain single sign-on to fail during this process:

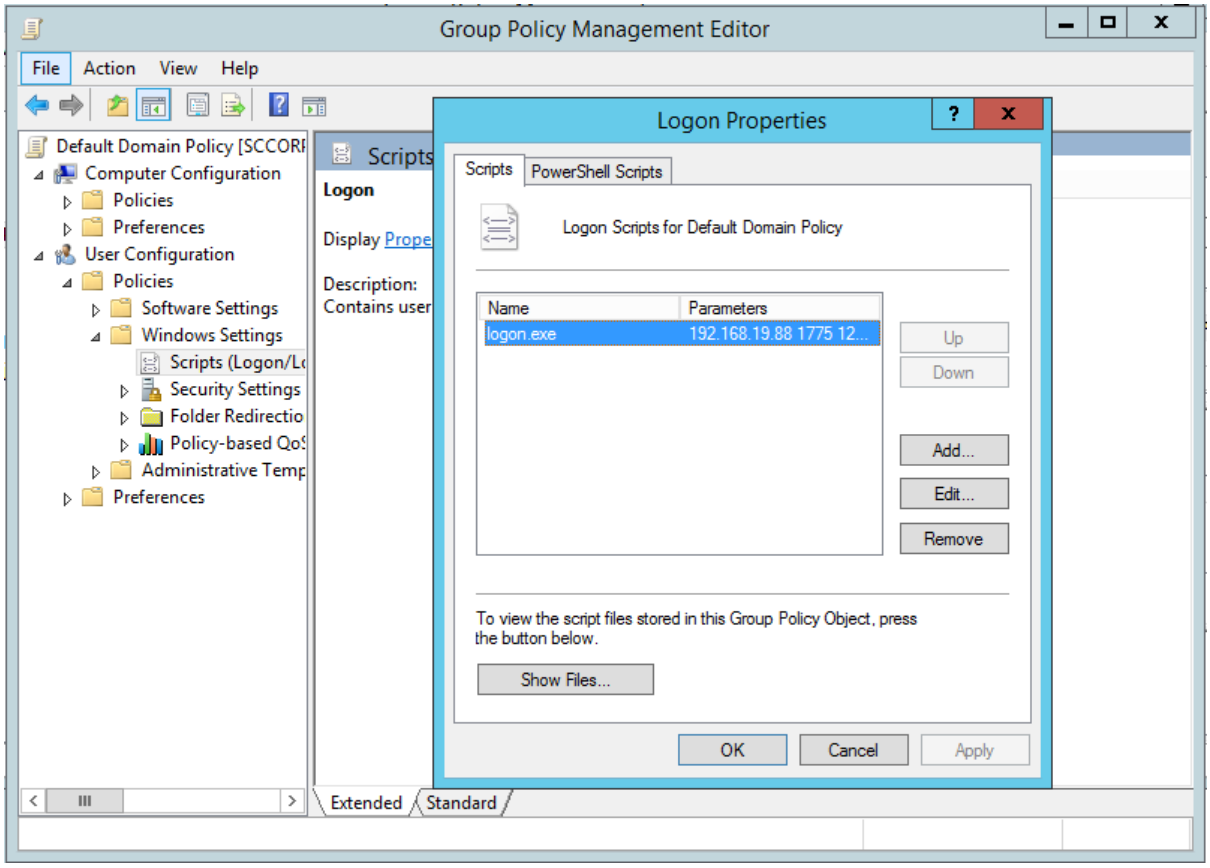
Is the single sign-on script on the AD domain server added and configured correctly?

Whether the domain group policy is successfully distributed to the PC?

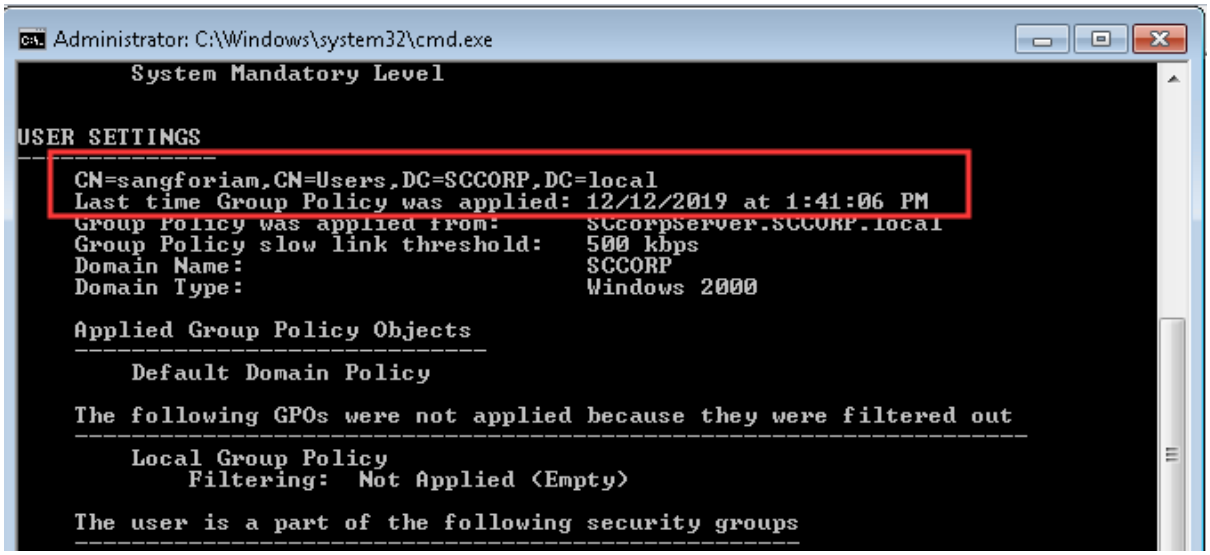
After the PC obtains the group policy, is it authorized to execute the logon.exe script?

1. Check the group policy settings on the domain server, if there is a corresponding domain account, use dsa.msc to view the user, and then see which ou the user belongs to; use gpmc.msc to view the entire domain or a group under one Policy, and then check its basic configuration.

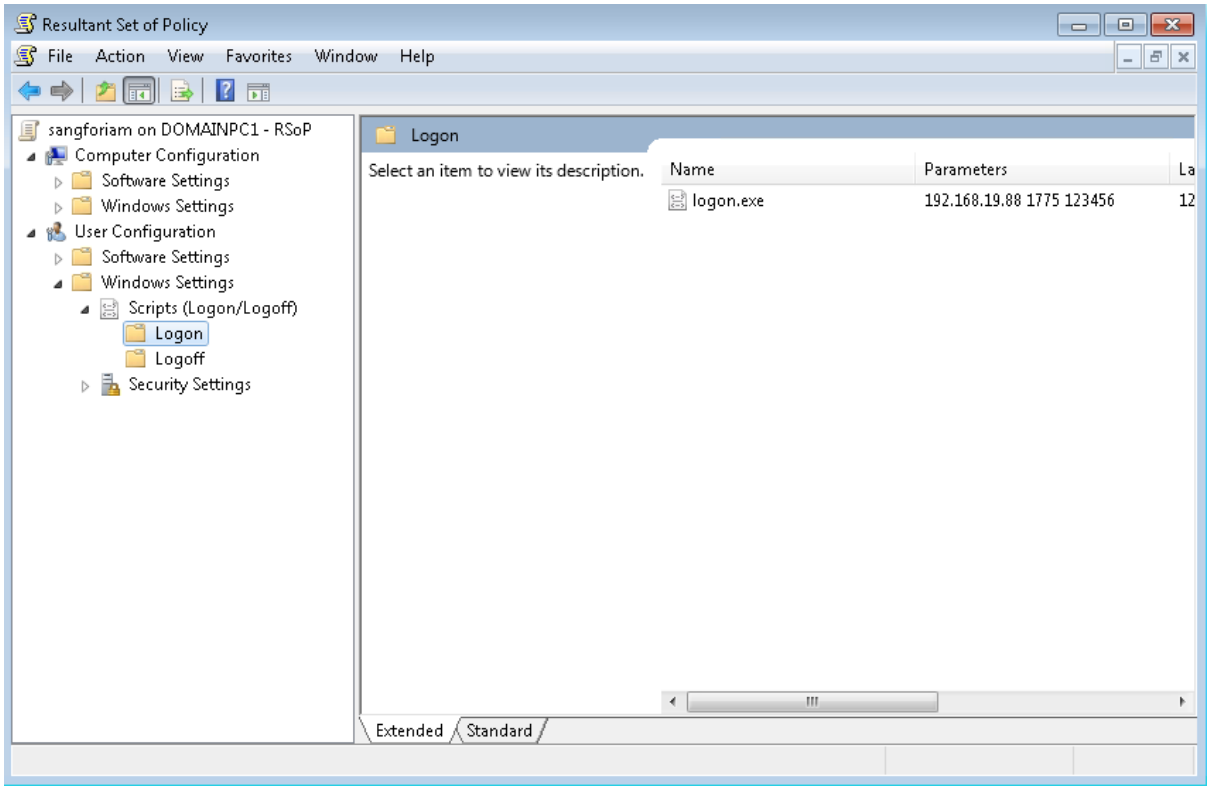

sangforiam Properties
Remote control
Remote Desktop Services Profile
COM+
General
Address
Account
Profile
Telephones
Organization
Member Of
Dial-in
Environment
Sessions
Member of:
Name
Active Directory Domain Services Folder
Administrators
SCCORP.local/Builtin
Domain Admins
SCCORP.local/Users
Domain Users
SCCORP.local/Users
Enterprise Admins
SCCORP.local/Users
Group Policy Cre...
SCCORP.local/Users
Netmon Users
SCCORP.local/Users
Schema Admins
SCCORP.local/Users
WseInvisibleToD...
SCCORP.local/Users
Add...
Remove
Primary group:
Domain Users
Set Primary Group
There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.
OK
Cancel
Apply
Help



2. Run the command "gpresult" or "rsop.msc" on the test PC to check whether the group policy matched by the PC is consistent with the configuration on the AD domain server. (gpresult is displayed on the command line, rsop.msc is displayed graphically)

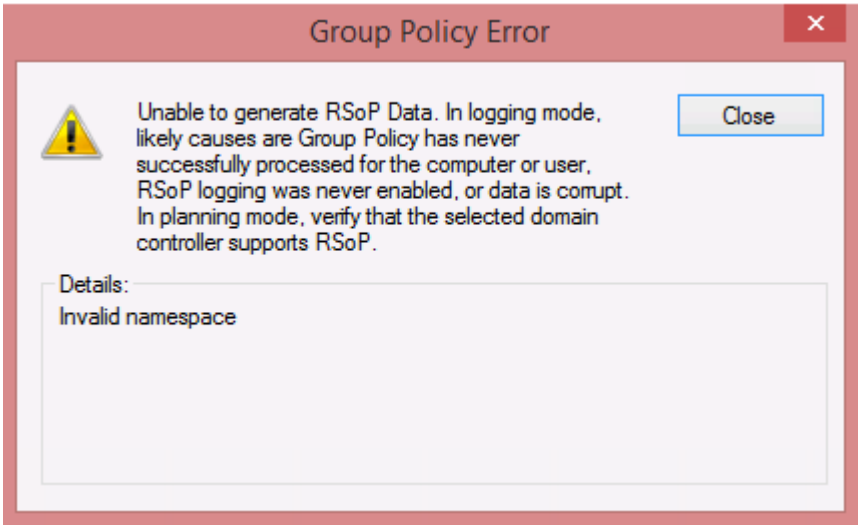


To confirm whether the current domain policy distribution is normal, you can use the rsop command to obtain the domain policy from the domain under normal circumstances, as shown below:

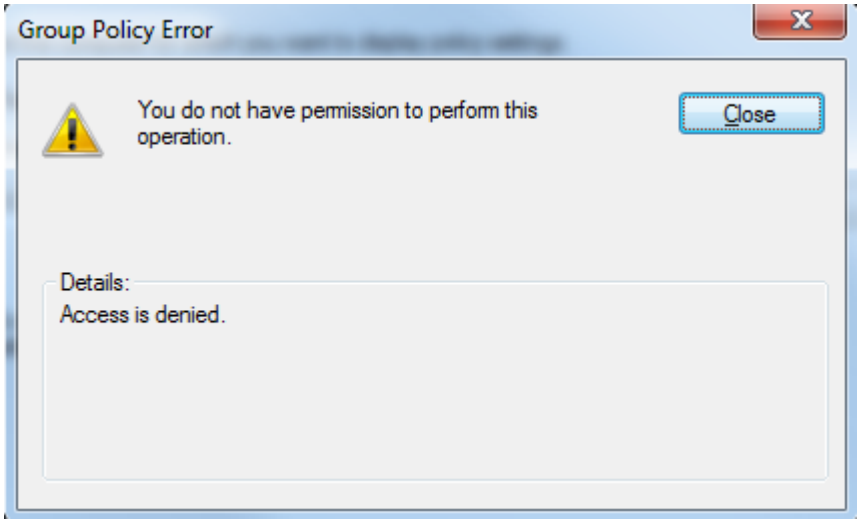


If there is a problem with the parameter check, you need to modify the parameters such as the IAM IP, default port, and shared key in the login script in the group policy. The shared key and the shared key configured on the IAM must be consistent.

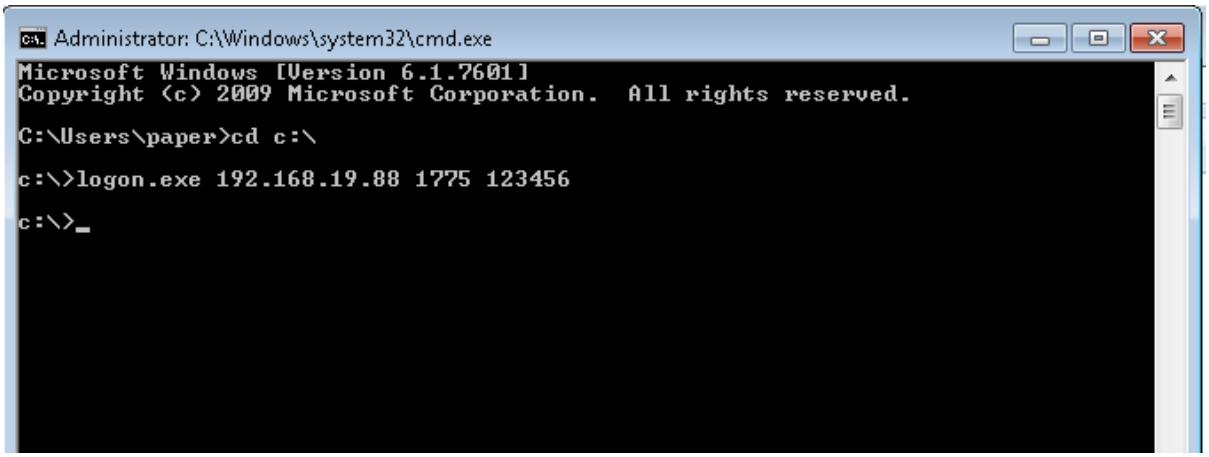
3. The group policy cannot be obtained using the rsop command. You need to check whether the group policy is lost.



4. When using the rsop command to prompt insufficient permissions, you need to add a domain user to the administratortoe group.

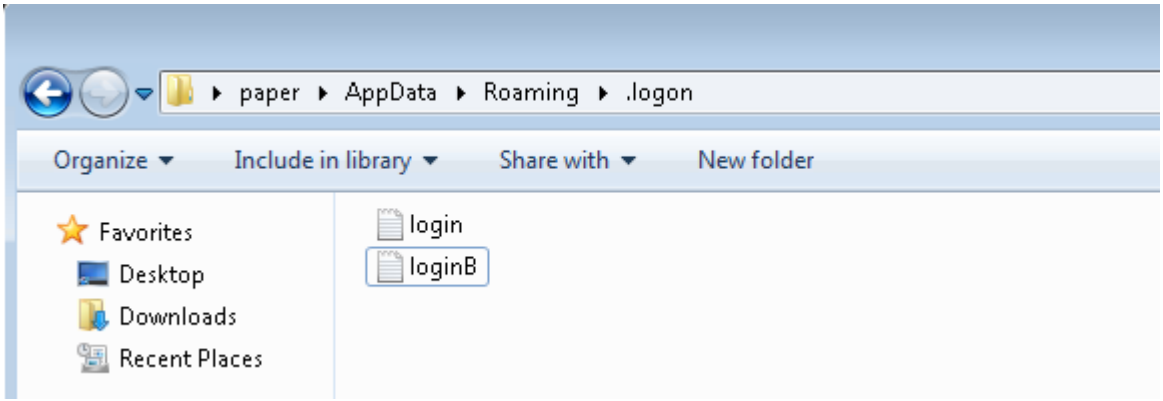


5.Manually execute the logon.exe script on the test PC, fill in the relevant parameters, and check whether the execution is successful.



3 PC runs logon.exe

1. After the PC successfully runs logon.exe, it generates a logon.txt log file (execute %appdata%/.logon) in the shared directory of the C drive of the PC (C: \ Documents and Settings \), and reports a successful login domain to IAM device (UDP1775).



Corresponding log error parameters:

reply: 401 magic error Shared Key error

reply: 402 Invalid ip IP or source IP is AC's IP

reply: 403 The user login on other ip IAM

reply: 404 The user is disabled

reply: 405 The user is expired

reply: 407 Dkey use The current user is a Dkey user

reply: 408 bind ip error The IP / MAC of the logged-in PC is bound by another user

reply: 500 Service stopped authd

reply: 500 (user, ip) is exis

reply: 501 Not allow new user

reply: IP or mac not in restrict range

During this process, the following factors can cause domain single sign-on to fail:

The domain account used by the PC to log in to the domain does not have write permission on the C drive shared directory

IAM single sign-on IP, port, and key set by domain group policy

The PC itself and the IAM cannot communicate with each other.

Based on the above factors that may cause SSO failure, the troubleshooting work we need to do is as follows:

1) Check that the domain account has read and write permissions to the C drive shared directory. You can manually create a file verification in the C drive shared directory.

2) Check if the logon.txt file is generated under %appdata% path

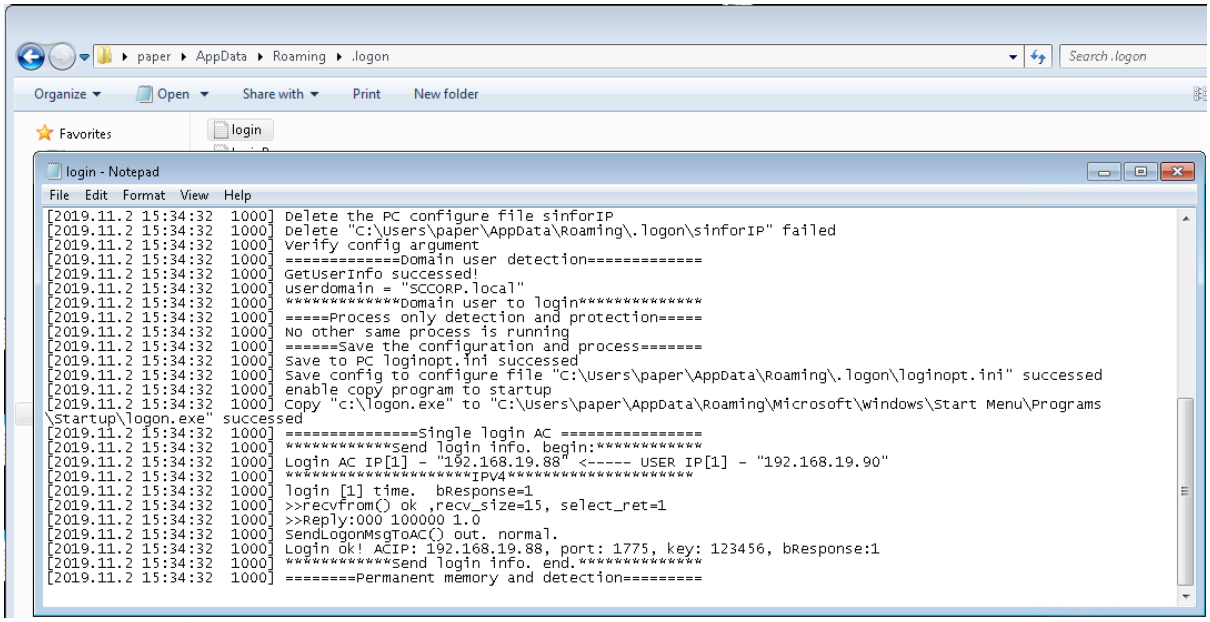
If you have read-write permissions but no logon.txt file is generated, you need to check whether the PC's local firewall or anti-virus software protects and prevents writing to the log file. You can turn off the local anti-virus software or firewall, and then log in to the domain to see if the logon.txt file is generated.

If the logon.txt file is generated and the domain single sign-on is unsuccessful, you can check the contents of the logon.txt file to see if the single sign-on is not successful due to a configuration problem, or if the PC sends a request to IAM without response

3) If the logon.txt file shows that the PC sends a message that the domain is successfully logged in to IAM, but IAM does not respond, you need to check whether the communication between the PC and IAM is normal and whether other network devices have intercepted the data packets. The most direct way is to grab the packet on IAM and see if the device can receive the single sign-on data packet sent from the PC.

4) In the same intranet environment, some PC single sign-on is successful and some PC single sign-on is unsuccessful, you can directly place the login script logon.exe locally on the computer that failed to log in, taking the C drive as an example , Execute in cmd : c:\ logon.exe IAM 's ip port key; if the test is successful, the network between PC and IAM is normal.

2. Open the %appdata% directory manually, check the log in the .logon file, and see the latest time processing.



The relevant error log is explained as follows:

Error Code	Reason
=ERR: Wrong number of parameters.=	logon.exe uses the command line method, and the number of parameters exceeds the maximum number of parameters
=ERR: can not get the module path=	Failed to get absolute path of logon.exe
=ERR: bad param format=	Parameters added after logon.exe are missing
=ERR: can not get the startup path or module path, Errorcode:	Usually because the domain user logs in for the first time, the user's environment directory is not ready, and the startup directory cannot be found
=ERR: can not get the PC sinforIP path=	Failed to get the configuration file sinforIP path
=ERR: can not get the domain sinforIP or PC sinforIP path=	Failed to get the path of the configuration file sinforIP on the domain or on the local PC
=ERR: can not get the loginopt.ini path=	Failed to obtain the loginopt.ini path, indicating that logon.exe is a command line execution mode and is offline
=ERR: Can not load	Loading configuration file failed
=ERR: %s - %d= %s represents the parameter, and %d represents the error code, which is generally 87, indicating that the parameter is illegal.	Illegal parameter, need to check the validity of the parameter

=ERR: %s - %d, use default value %d=	Failed to get parameters, adopt default value
=ERR: prepare data failed, ERR_Line:	Failed to obtain IAM IP or local IP
=ERR: Login Failed! ACIP: %s, port: %d, key: %s, bResponse:%d=	Logon Failed
=ERR: Encrypt message failed, ret:	Failed to encrypt sent data (login or logout or heartbeat)
=ERR: Send heart beat to AC \"%s\" failed: %d=	Failed to send heartbeat packet
=ERR: >>Login Failed! port: %d, key: %s=	Failed to send login package
=ERR: >>Logoff failed: %d=	Failed to send logout packet
=ERR: SockInit() failed:	Failed to initialize the socket.
=ERR: Timeout=	No reply packet is received, the IP of the IAM that may be sent does not exist, and the firewall may be enabled under win7
=ERR: CreateDirectoryW failed:	Failed to create log directory
=ERR: CryptQueryObject failed:	Failed to get digital signature. In this case, logon.exe enables digital signature detection.
=ERR: CertFindCertificateInStore failed:	Failed to obtain the signing certificate. In this case, logon.exe enables digital signature detection.
=ERR: CreateThread for IP detection failed:	IP change detection thread creation failed
=ERR: to OpenProcess %d terminate: %d=	System error, try to log in again
=ERR: to terminate process:	Failed to kill the specified process
=ERR: OpenProcessToken failed:	Failed to open token handle while getting user information
=ERR: GetTokenInformation failed: or=ERR: LookupAccountSid failed: or=ERR: GetTokenInformation failed: or=ERR: GetUserName failed:	Failed to open token handle while getting user information

Chapter 2 Common issue

2.1 Users intermittently go online and offline on IAM

1. The network between PC and IAM is unstable

Troubleshooting steps

Open the console on IAM and enter ping X.X.X.X -t (X.X.X.X is the IP of IAM)

If packet loss occurs, implement the solution

Solution:

Reduce the repeated login interval (depending on the situation, this problem cannot be solved fundamentally, it can only reduce the probability of its occurrence)

2.The IAM timeout without traffic logout time is less than the repeated login cycle time

Troubleshooting steps

View the timeout period of no logout on the IAM a

View the repeated login cycle b in the logon configuration file

Solution

Modify the timeout of no timeout to a larger point to make it longer than the repeated login time period or close the timeout of no timeout

2.2 Domain users go online in IAM but cannot access the Internet

1. IAM cannot connect to the Internet

Troubleshooting steps

First check whether it is a problem other than IAM. Open the pass-through on IAM. If you are online, go to the next step.

Enter the IAM background through the background

Run the ping command, ping 8.8.8.8 or ping www.baidu.com, if the ping fails, implement the solution

solution

Solving IAM Network Problems

2. The specified user or group cannot be connected to the Internet in the IAM Internet policy

Troubleshooting steps

First check whether it is a problem other than IAM. Open the pass-through on IAM. If you are online, go to the next step

Check the IAM Internet access strategy and check whether the Internet access restriction policy includes users who have failed to access the Internet.

solution

Modify Access Control management.

3.Online user's IP non-communication IP

Troubleshooting steps

Check that the IP of the online user and the IP of the IAM are not on the same network segment

logon allows multiple IPs to go online, and IAM is configured to log off old IPs when authentication conflicts

After the above two conditions are met, implement the solution

solution

Modification method 1: Logon configuration allows only single IP to go online

Modification method 2: IAM configuration does not log off the old IP when authentication conflicts

2.3 Domain users are not online on IAM but the logon process is running on the PC

1. PC and IAM cannot communicate directly

Troubleshooting steps

Ping IAM on the PC. If the ping fails, implement the solution.

Solution:

It may be that the IAM has disabled the user's DNS function. On the IAM interface, enable access to the DNS service.

Make the PC have an IP and IAM IP on the same network segment, and the gateway configured IP is the IAM IP

2. The configuration file has errors

Troubleshooting steps

Check the configuration file information. Check whether the IP of IAM and the IP of DNS match the real ones. If not, implement the solution.

Check the logs to see if there are 87 error codes, and if so, implement the solution

Check the log, if the last IAM IP sent is 3.4.5.6, the configuration file is wrong, then implement the solution

Solution:

Modification method 1: Write the real IAM IP or DNS IP

Modification method 2: Go through the configuration file again and remove the extra spaces

Modification method 3: reconfigure and deploy the default configuration file according to the desired configuration

3. The new logon was not successfully deployed and the new sinforIP did not take effect.

Troubleshooting steps

Compare the sinforIP on the domain, the local sinforIP and the final backup configuration file loginopt.ini. If there are differences, implement the solution.

Solution:

Compare the sinforIP on the domain, the local sinforIP and the final backup configuration file loginopt.ini. If there are differences, implement the solution.

4. The network is not good and the duplicate login function is not enabled.

Troubleshooting steps

Ping the IP of IAM on the PC

If the result is intermittent, then implement the solution

Solution:

In this case, the network is generally not good. After the timeout and no traffic logout, the user does not go online in time.

Enable the repeated login function in the logon configuration. Set the repeated login period as small as possible.

2.4 Domain users are not online on IAM and no logon process is running on the PC

1. Non-domain user login

Troubleshooting steps

Under the XP system, before the user logs in, you will be asked to choose whether to log in locally or in the domain. If you log in locally, you will implement the solution.

Under win7 system, the user is logged in as a local user by default. If you want to log in to the domain, write the domain name in front of the user name, separated by "\"

Solution:

Under xp system, please select the domain and login with username

Under Win7 system, you should also add the domain name in front of the user name. If the local user name is the same as the domain user name, it will be entered as a local user by default.

2. Domain user login failed

Troubleshooting steps

Domain and PC did not update Group Policy

Multiple group policies are configured on the domain and interfere with each other

TCP / IP NetBIOS Helper service on the domain or PC is not enabled or set to manually enabled

Solution:

Just execute gpupdate and gpupdate / force on the domain and log in to the domain again

Interference in multiple policies, delete unnecessary group policies

Start the service TCP / IP NetBIOS Helper and set the startup mode to automatic startup. Enter services.msc in the command line to view the system service startup status and start the service TCP / IP NetBIOS Help.

Chapter 3 Precautions

1. The default authentication port used by version 6 before IAM 11.0 is 1773, and 11.X is 1775

2. Go back to **Logon Properties** window, click **Add** to add **logon.exe** script into script list and specify script name and parameters. If **Script Parameters** field is null or configured with only one parameter, the configuration file **sinforIp** is required to be added to script list; otherwise, it is not required. The following introduces four formats of script parameters:

Without parameter (recommended)

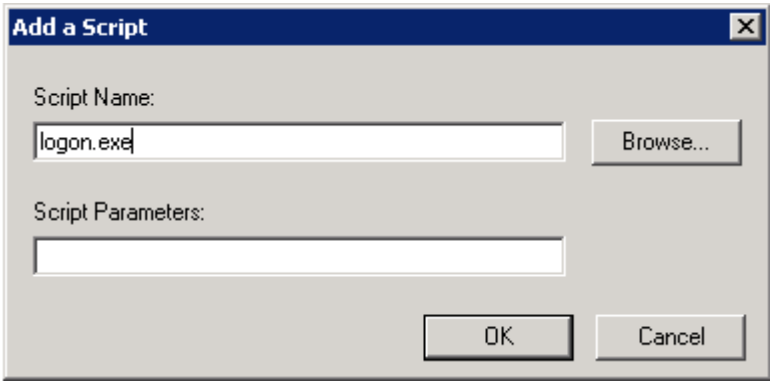
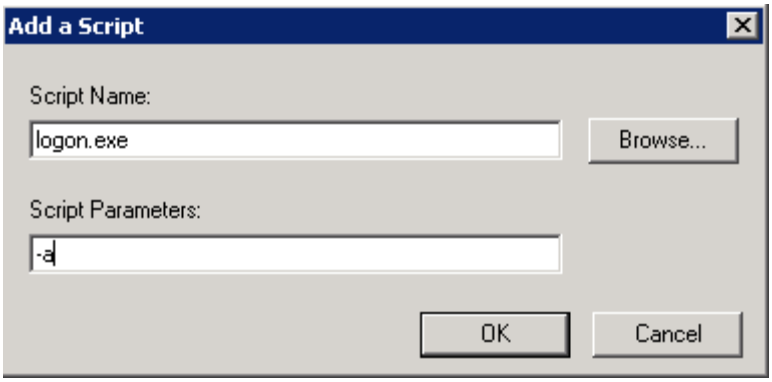


Figure 7 Without Script Parameter

3. With parameter **-a**

If the parameter is set to **-a**, user can use the configuration file pushed from the domain controller. **-a** indicates that number of attempts that login profile is sent is default. Therefore, login profile will be sent to the IAM device specified times without need to wait response packets from that device when user logs in to the domain.



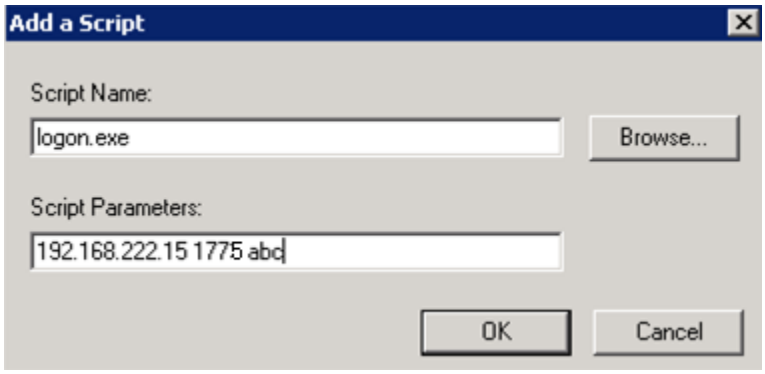
With parameter **-a**

4. With parameters in format of **Value1 Value 2 Value 3** (separated with space).

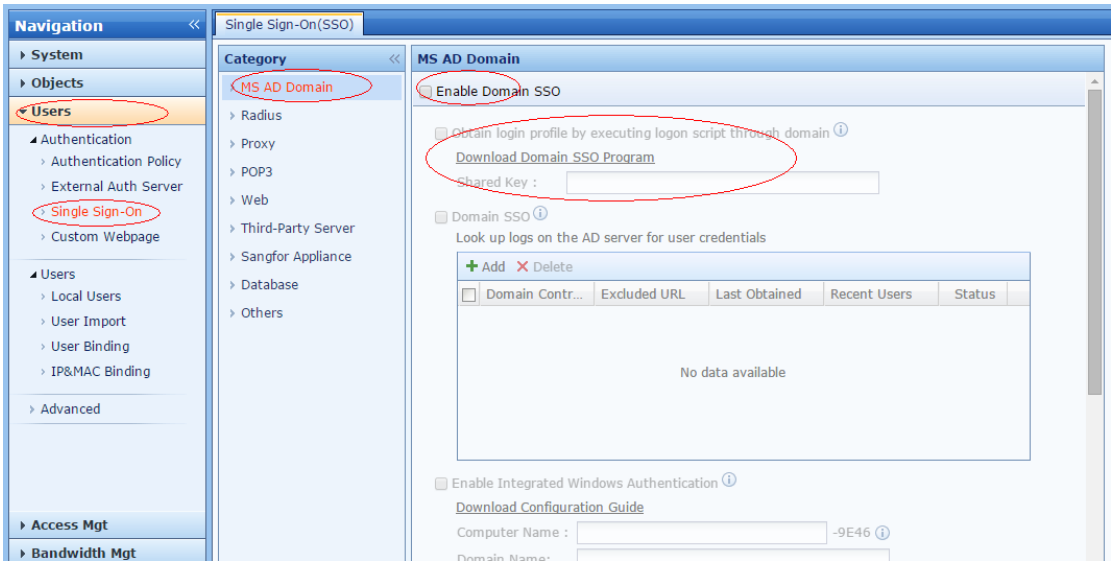
Value 1: Indicates the IP address of IAM unit

Value 2: Indicates the listened port on IAM unit(1775, unchangeable)

Value 3: Indicates the communication key which should be the same as the shared key specified on Web admin console of the IAM unit, as shown in Figure 10.

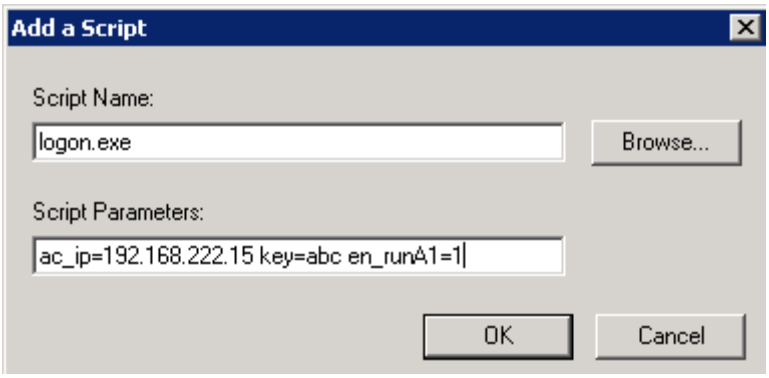


Parameter in the third format



Shared Key on IAM Unit

5. With parameters in format of **Title1=value1 Title 2=value2... Title15=value15** (up to 15 parameters separated with space), as shown in Figure 11.



Parameters in the fouth format

The table below introduces the available parameters:

Script Parameters

CMD Line Parameter	Parameters in Config File	Value	Unit	Default	Range	Remarks
en_runAl	EnableRunAlways	0, 1	---	1	0, 1	It it is set to 1, it indicates logon.exe program is always running after startup; otherwise, it will exit after being executed once.
en_ckSign	EnableSignature	0, 1	---	0	0, 1	Decides whether to enable digital signature verification (for checking process).
en_repeatL	EnableRepeatLogon	0, 1	---	0	0, 1	Decides whether to send login profile repeatedly(if enabled, IAM unit will not log off user automatically when internal network connection error occurs).
en_copyStart	EnableCopyStartup	0, 1		1	0, 1	Decides whether to copy logon.exe program to Startup folder
baklogP	BaklogPath	Null or valid path	---	Null	Null or valid path	If default path %appdata% has no write permission, logs will be stored in given path (it can only have level-one folder). If specified path has no write permission, default path will be used to store logs.
en_heartB	EnableHeartBeat	0, 1	---	0	0, 1	Determines whether to send heartbeats to IAM unit(If enabled, IAM unit logs off user if no heartbeat is received even though logoff script fails to be executed).
en_response	EnableResponse	0, 1, 2	---	2	0, 1, 2	Check if user logs in to IAM unit based on response packet.

en_logon_AIP	LogonALLIP	0, 1	---	0	0, 1	Decides whether to enable user to log in to IAM unit on different IP addresses (it applies to the situation that one PC owns multiple IP addresses).
en_logoff_OIP	LogoffOldIP	0, 1	---	0	0, 1	Decides whether to log off logon session from current IP address when user logs in to IAM unit on a new IP address.
ac_ip	sinforIP	Valid IP address	---	3.4.5.6	0.0.0.0~255.255.255.255	IP address of IAM unit
key	shareKey	ASCII characters	---	123	Up to 23 characters	Shared key (case-sensitive, special characters supported)
port	Port	1775	---	1775	1775	Port number(fixed value)
reLogon_I	RepeatLogonInterval	Positive integer	Sec	180	[10,1000]	Logon interval
heart_beatI	HeartBeatInterval	Positive integer	Sec	30	[10,50]	Interval that heartbeats are sent again
checkIP_I	CheckIPInterval	Positive integer	Sec	10	[1,100]	Interval that IP address is checked again.
timeout	ResponseTimeOut	Positive integer	Sec	5	[1,50]	Timeout that logon.exe program waits response packets.
retry_times	RetryTimes	Positive integer	Times	3	[1,20]	Number of attempts that login profile is sent.
	Generally, process is verified through username, process name and signature. But Logon.exe signature becomes invalid if it is downloaded via Web browser, you can configure parameter en_ckSign to decide whether to enable digital signature verification (Default en_ckSign indicates that digital signature verification is not enabled) If Script Parameters field is set to -a, login profile will be sent to IAM device three times without need to wait response packets from that device; if that parameter is not -a and logon.exe program is configured to not check whether user logs in to IAM unit based on response packet, login profile will be sent to IAM device for given times based on the value of parameter RetryTimes. If parameter en_heartB is set to 1, login profile will be sent to IAM device repeatedly (en_repeatL=1). Note:					

	If parameter en_heartB is set to 1, heartbeat detection feature should be enabled on IAM unit. To enable it, add the field bAutoHeartBeat = 1 under Option field in configuration file authoption.in of IAM unit. Restart the process authd after saving changes to that file. Value of parameter checkIP_I cannot be greater than that of parameter reLogon_I; otherwise, parameter checkIP_I will be set to the maximum of parameter reLogon_I minus 1 automatically. Value of parameter heart_beatI cannot be greater than that of parameter reLogon_I; otherwise, parameter heart_beatI will be set to the maximum of parameter reLogon_I minus 1 automatically.

6. Every time you modify Group Policy or replace logon.exe on the domain, you must update the Group Policy again. gpupdate and gpupdate /force.

7. When there are multiple IAMs, you need to configure sinforIP.

Configuration file in new format is designed to meet various scenarios and provide more complete configuration. Domain administrator can specify relevant parameters. The configuration file as described in table 4 is a simple example.

Configuration file in new format

```
[LogonCtrl]
EnableRunAlways = 1
EnableSignature = 0
EnableRepeatLogon = 0
RepeatLogonInterval = 180
BaklogPath =
EnableCopyStartup = 1

[HeartBeat]
EnableHeartBeat = 0
HeartBeatInterval = 30

[Response]
EnableResponse = 2
ResponseTimeOut = 5
RetryTimes = 3

[CheckIP]
LogonALLIP = 0
LogoffOldIP = 0
CheckIPInterval = 10

[AC]
ACMax = 200
ACCount = 0

[AC1]
sinforIP = 192.168.31.190
```

```
Port = 1775
shareKey = abc

[AC2]
sinforIP = 192.168.31.198
Port = 1775
shareKey = 123
```

SANGFOR