SANGFOR

NGAF

AD Domain SSO Configuration Guide

Version 8.0.10

Change Log

Date	Change Description
October 21, 2019	AD Domain SSO Configuration Guide.

CONTENT

Chapter 1 Abbreviations and conventions 1
Chapter 2 Demand background 1
Chapter 3 Application method 2
Chapter 4 Testing Environment 3
4.1 Testing topology 3
Chapter 5 Testing Result 4
Chapter 6 Precaution 5
Chapter 7 Attachment A 6

Chapter 1 Abbreviations and conventions

AD domain: Windows Active Directory

Integrated Windows authentications: A scheme for single sign-on referred to as IWA

Domain Monitoring Single Sign-On: One option for single sign-on is the old version of the ADSSO solution.

Listening mode Single sing-on: A scheme for single sing-on, listening to the data of the computer login domain and obtaining the information of the login domain.

Gpupdate.EXE /FORCE: Refresh the group policy command. After changing the group policy, you need to execute this command to make the changes take effect immediately.

Rsop.msc: Execute on the PC that is added to the domain. You can use this command to check whether the PC obtains the domain group policy.

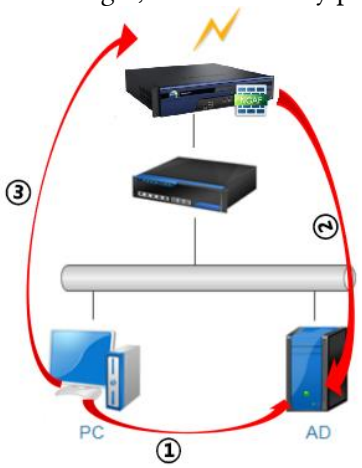
Gpresult.exe: Report on the PC joined to the domain. You can use this command to check whether the PC obtains the group policy of the domain.

Chapter 2 Demand background

1. AD domain single sign-on is applicable to the intranet of the customer. The intranet has been configured to manage the intranet users. After the AC is deployed, the AC and the AD domain are required to implement the smooth authentication. Authentication online, no need to manually pass AC certification, transparent to end users)
2. I want to use the real name of the domain user to access the Internet, and the real name records the user's online log.
3. The client does not want to use script mode to single sign-on, because the script mode needs to configure logon.exe and logoff.exe on the domain, which does not comply with the company's security management specifications.
4. In order to improve the success rate of single sign-on, in the actual scenario, it is necessary to integrate Windows authentication, domain monitoring single sign-on and monitoring mode. The three single sign-on solutions are enabled together. It is not recommended to enable any one of them separately. Introduce the usage of these three programs.

Chapter 3 Application method

Domain monitoring single sign-on, that is, the old version of ADSSO, the NGAF automatically detects the event log of the user's login domain on the AD domain (event ID is 672, 540, 4624). After detecting the log of the user login, it automatically passes the NGAF's authentication.



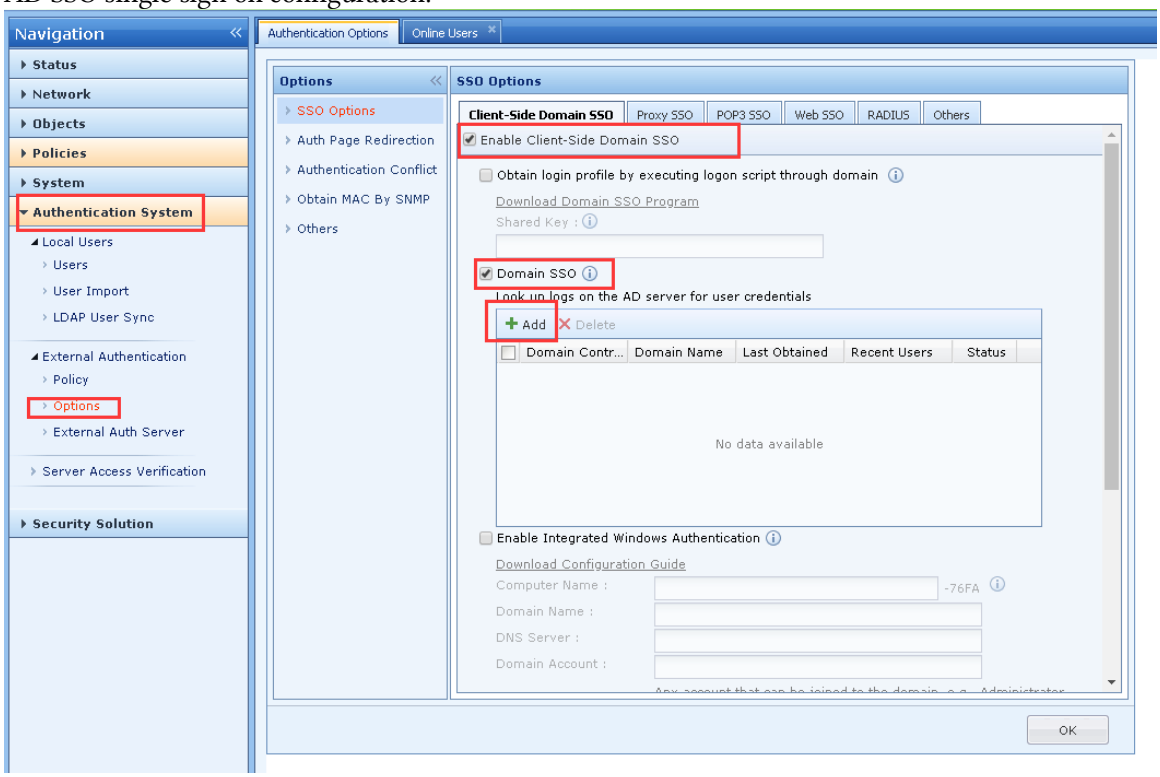
1. PC logs into domain.
2. Agent communicate with AD server to obtain domain online users' information.
3. PC is authenticated and able to access Internet.

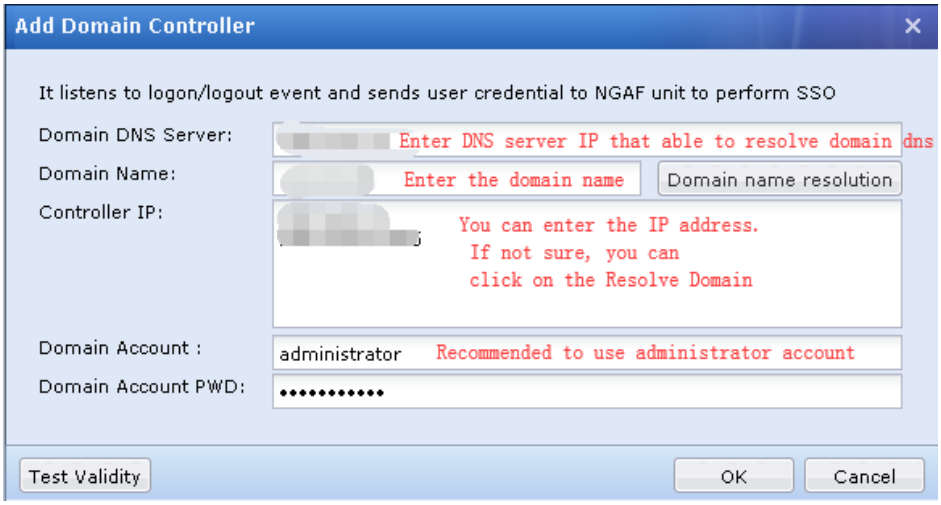
Chapter 4 Testing Environment

4.1 Testing topology

A common test environment, device routing or bridge deployment, and AD domain deployment on the intranet switch, as shown in the following figure. This article mainly introduces the test method of script single point login in this environment.

AD SSO single sign on configuration.





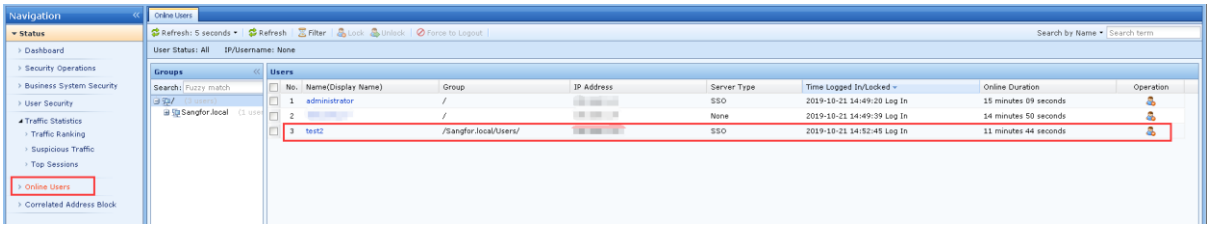
Note: Figure above recommend to use the administrator account, if is using windows 2008 and above, you also can use non-administrator account, but you need to assign wmi-permission.

If non-administrator account, please refer to attachment A.

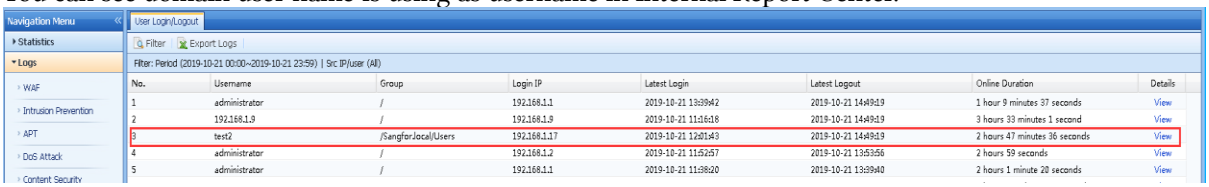
Chapter 5 Testing Result

Result of single sign on as below.

1. User logon PC and login into domain, it will automatic pass the NGAF's authentication, it no need open the web browser to authenticate again, in Online users list, you can view the user is using SSO online, as below.

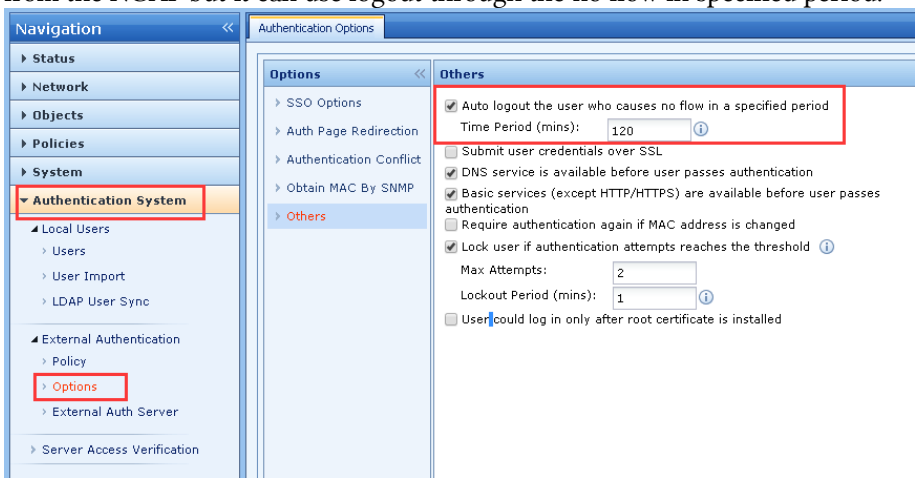


2. You can see domain user name is using as username in Internal Report Center.

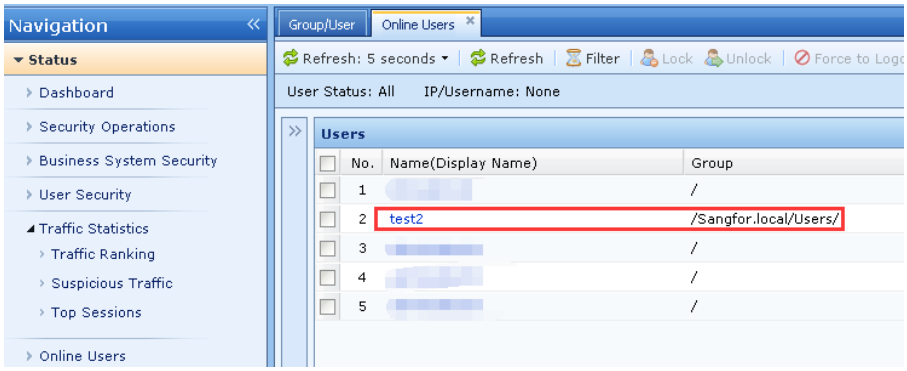


Chapter 6 Precaution

1. Domain SSO, IWA and listening mode not support domain SSO sign off from the domain and offline from the NGAF but it can use logout through the no flow in specified period.



2. Domain SSO, endpoint device must pass through NGAF then only can go online (can view in online user list), the program will check for every 10 minutes, if does not have traffic pass through, it will not show the user is online in online user list.

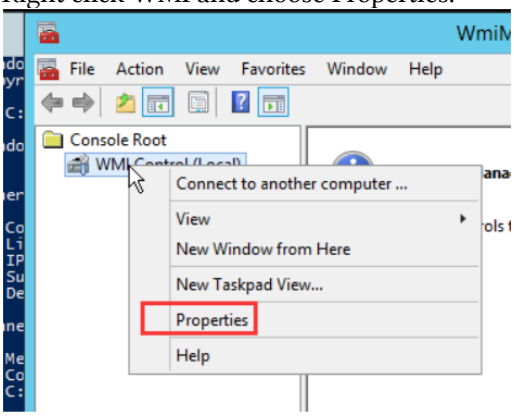


3. If the AD is at the WAN side, endpoint PC unable login to domain, it required to put the AD domain server's IP address to the NGAF's Global Exclude list to do open auth and allow the AD communication.

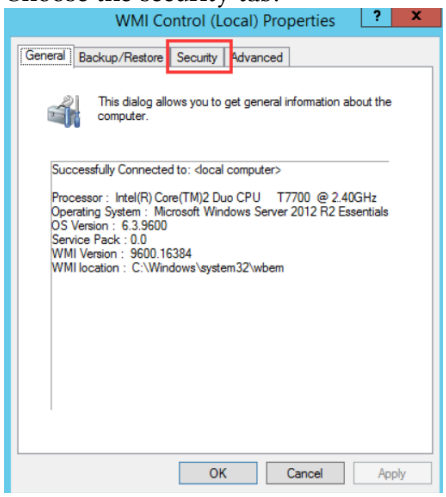
Chapter 7 Attachment A

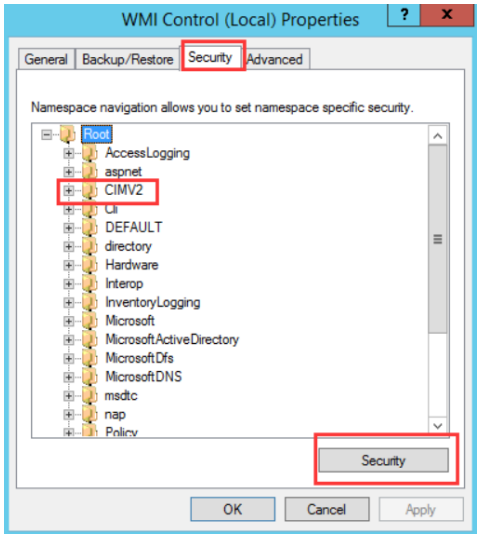
Windows server 2008 AD domain non-administrator account configuration. If it is windows server 2008 and above domain cotroller, it can use the non-administrator account, but it required to assign WMI permission, configuration guide as below:

1. Go to start -> run and type wmingmt
2. Right click WMI and choose Properties.

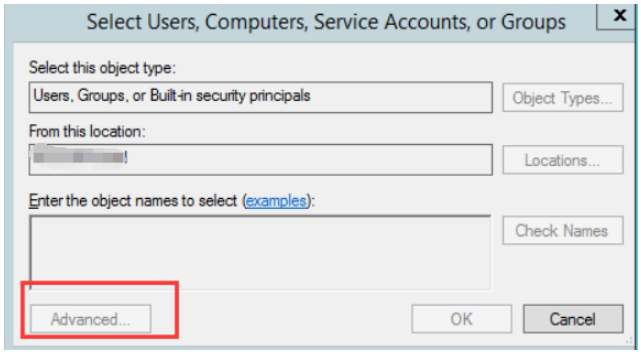


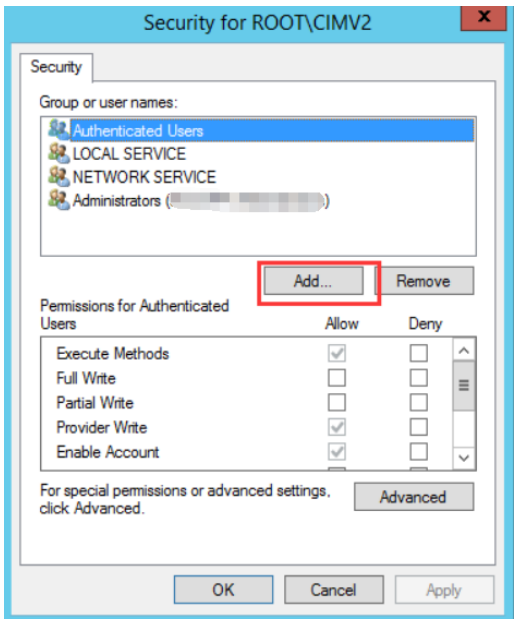
3. Choose the security tab.

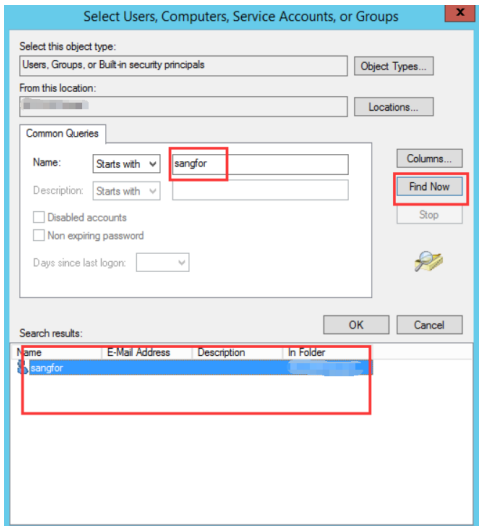




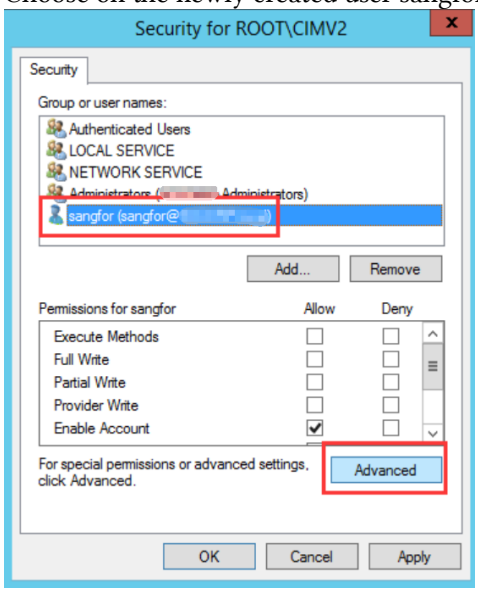
4. Click on add.

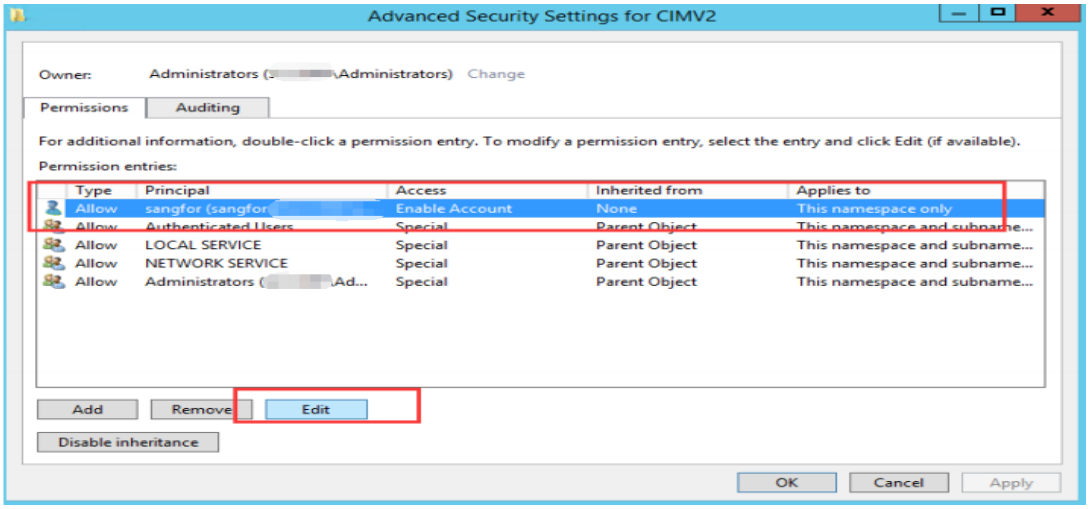

Select Users, Computers, Service Accounts, or Groups
Select this object type:
Users, Groups, or Built-in security principals
Object Types...
From this location:
Locations...
Enter the object names to select (examples):
Check Names
Advanced...
OK
Cancel

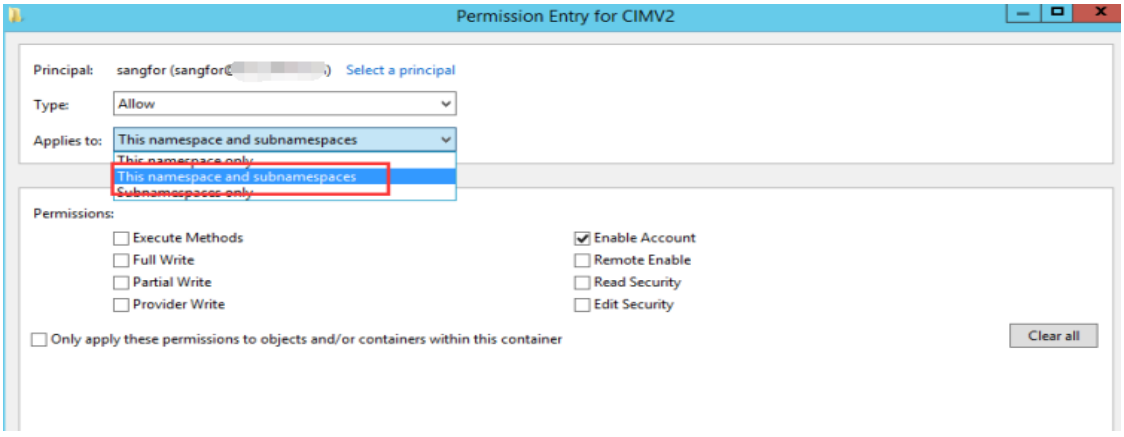

Security for ROOT\CIMV2
Security
Group or user names:
Authenticated Users
LOCAL SERVICE
NETWORK SERVICE
Administrators (
Add...
Remove
Permissions for Authenticated Users
Allow
Deny
Execute Methods
Full Write
Partial Write
Provider Write
Enable Account
For special permissions or advanced settings, click Advanced.
Advanced
OK
Cancel
Apply


Select Users, Computers, Service Accounts, or Groups
Select this object type:
Users, Groups, or Built-in security principals
Object Types...
From this location:
Locations...
Common Queries
Name:
Starts with
sangfor
Description:
Disabled accounts
Non expiring password
Days since last logon:
Columns...
Find Now
Stop
OK
Cancel
Search results:
Name
E-Mail Address
Description
In Folder
sangfor

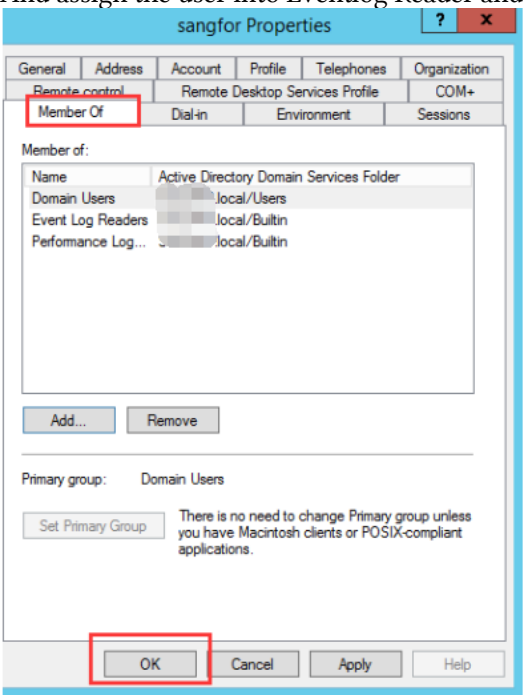
5. Choose on the newly created user sangfor.







6. And assign the user into Eventlog Reader and Performance log user group as below :



7. So the windows 2008 AD domain non-administrator already configured, domain SSO can use this account.

SANGFOR