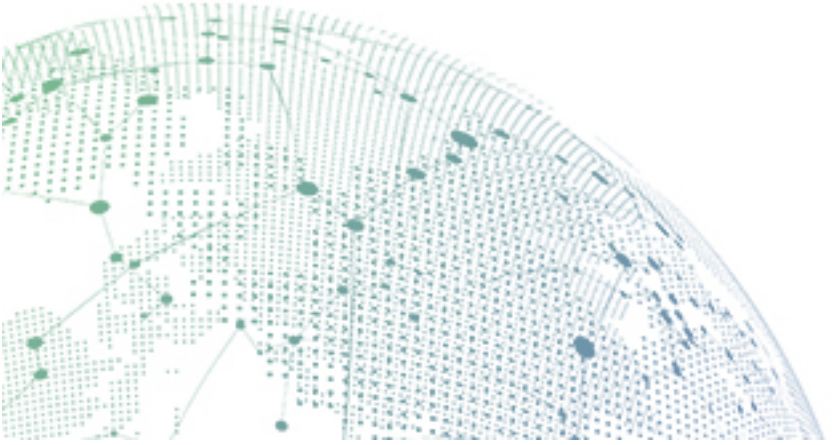
SANGFOR

NGAF

IWA Single Sign-On Configuration

Version 8.0.5



Change Log

Date	Change Description
Nov 5, 2018	Version 8.0.5 document release.

CONTENT

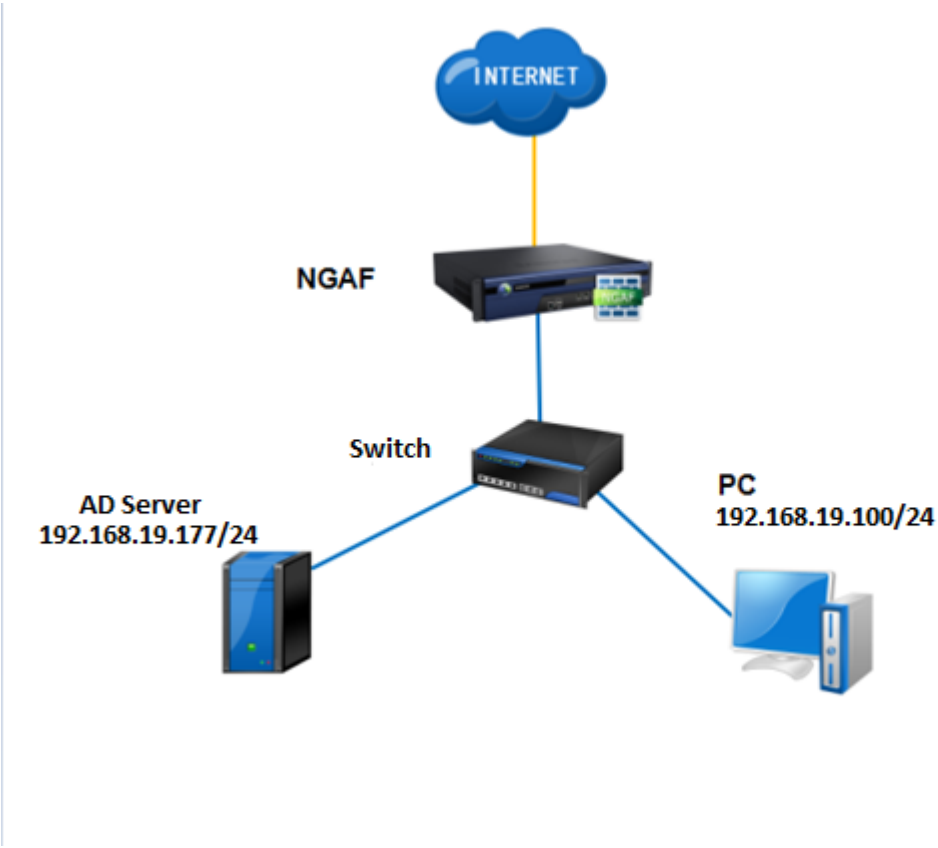
Chapter 1 IWA SSO Introduction

On the intranet, there is a domain controller for management. After the NGAF device is deployed, the IWA can be configured for single sign-on. After the user PC is logged in to the domain account, the PC is authenticated as the domain user by NGAF and obtain internet acces. The NGAF can query the related log records of the domain user.

Configure IWA single sign-on, no need to change any settings of the domain server, nor need to install software on the PC, the configuration is simple and fast, and the impact on the customer network environment is small.

Chapter 2 Application Scenario

Application Scenario for IWA Single Sign-On



NGAF deployed as route/bridge/virtual wire at WAN, configure IWA Single Sign-On function to authenticate LAN user. Relevant security policy can be configured based on authenticated user.

In this test environment, the NGAF is deployed as routing mode. The address of the AD server is 192.168.19.177/24, and the domain cti.sangfor.com is established. The IP address of the PC is 192.168.19.100/24. The PC has joined the domain.

Chapter 3 Essential Element

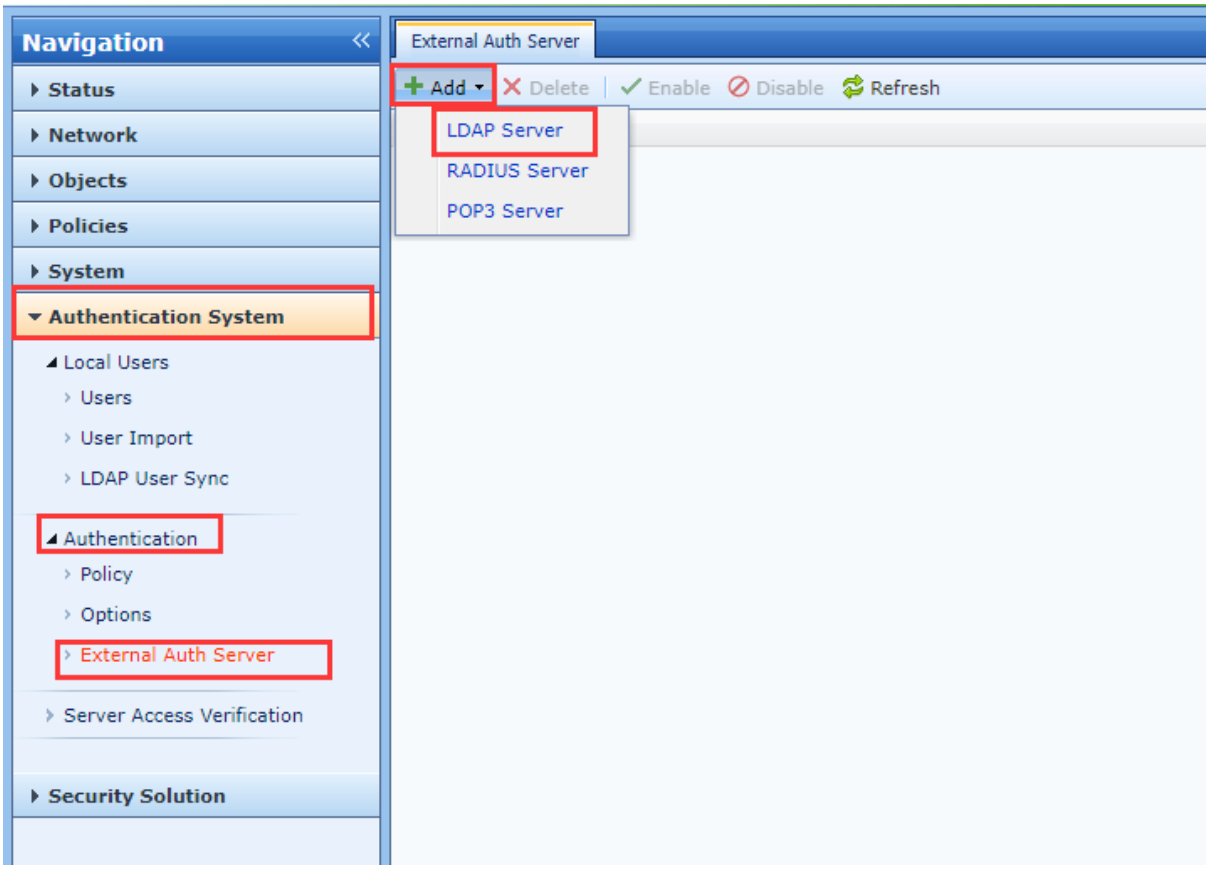
1. The data traffic of the PC Internet access must pass through the NGAF device.
2. NGAF can communicate with the domain server normally.
3. IWA authentication, the PC needs to exchange data packets with the NGAF 1.1.1.2 address to ensure that the PC accesses the 1.1.1.2 packet through the NGAF

Chapter 4 Configuration Idea

1. Configure LDAP server.
2. Configure LDAP Automatically Synchronize.
3. Configure Single Sign-On.
4. Configure IWA Single Sign-On authentication policy.

Chapter 5 Configuration

1. In **Authentication System** > **Authentication** > **External Auth Server**, Select **Add** > **LDAP Server**.



2. Enter the credential as shown below.

   Name : iwa

   Address : 192.168.19.177

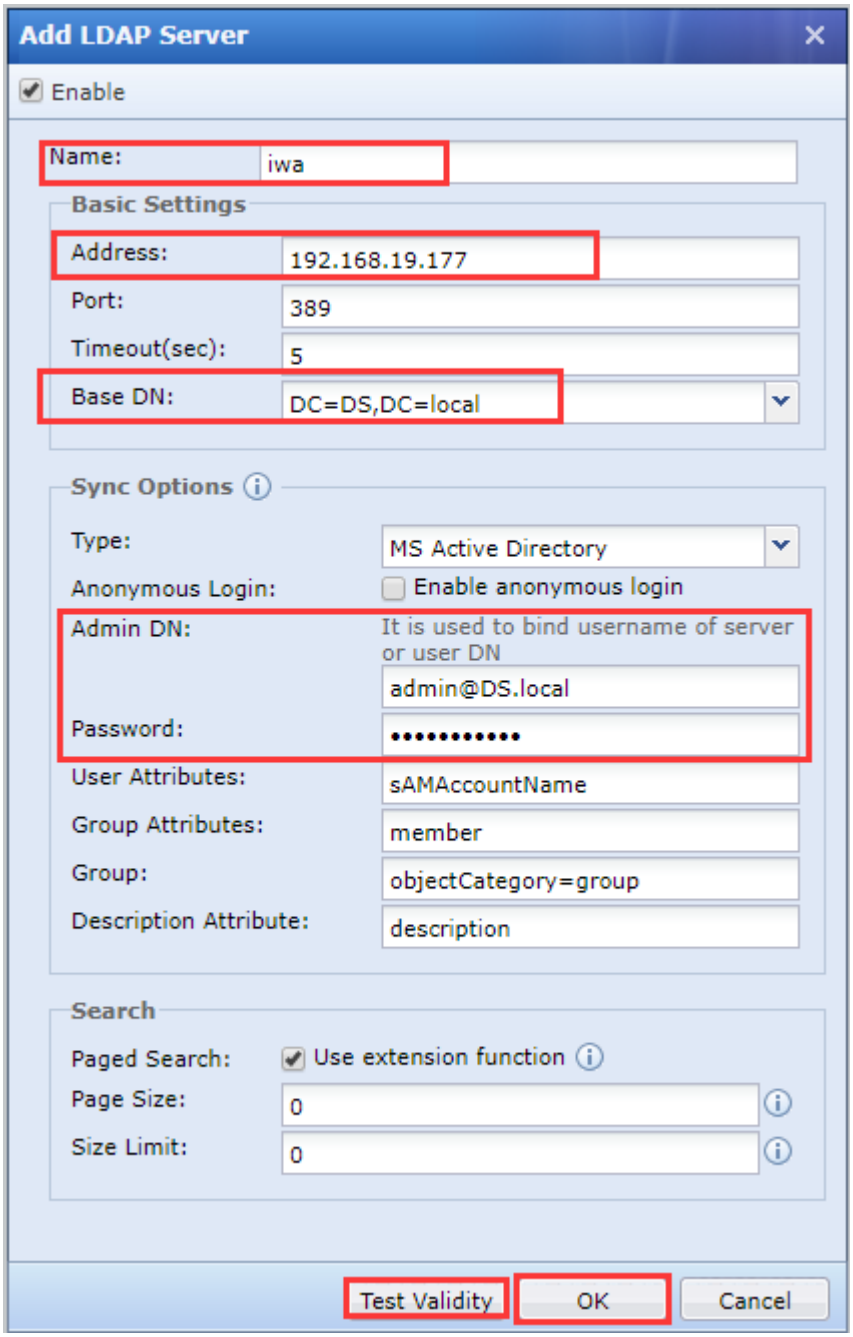
   BaseDN : DC=DS,DC=local

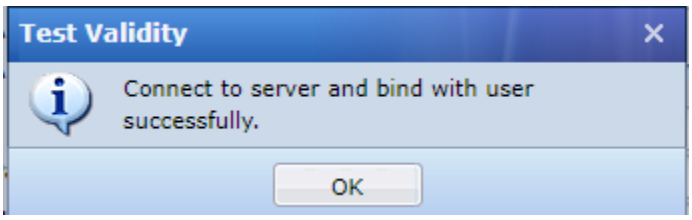
   Admin DN : Domain username with privilege

   Password : Password of the domain username entered in Admin DN

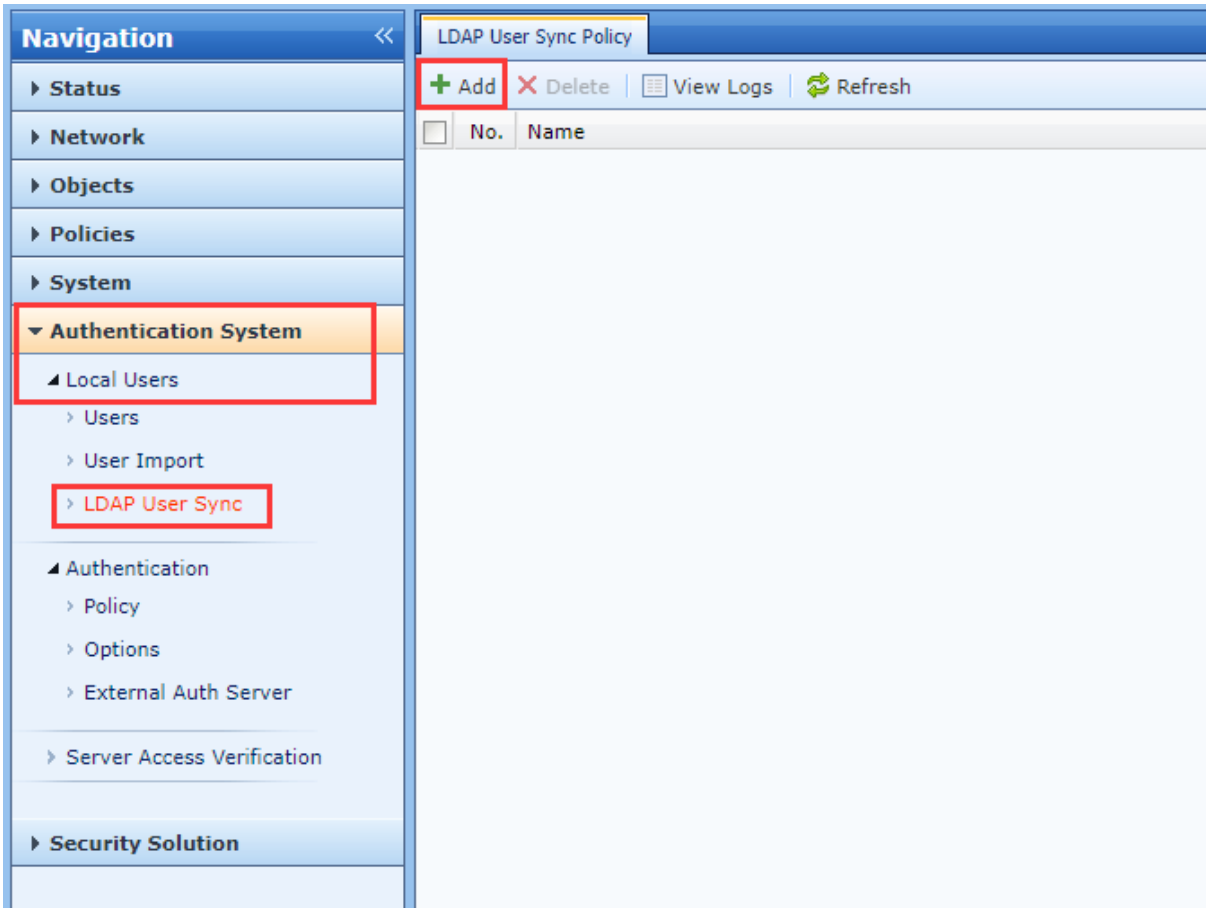
   Click on the Test Validity and prompt “Connect to server and bind with user successfully“ which represent all configuration are correct.

   Click OK.

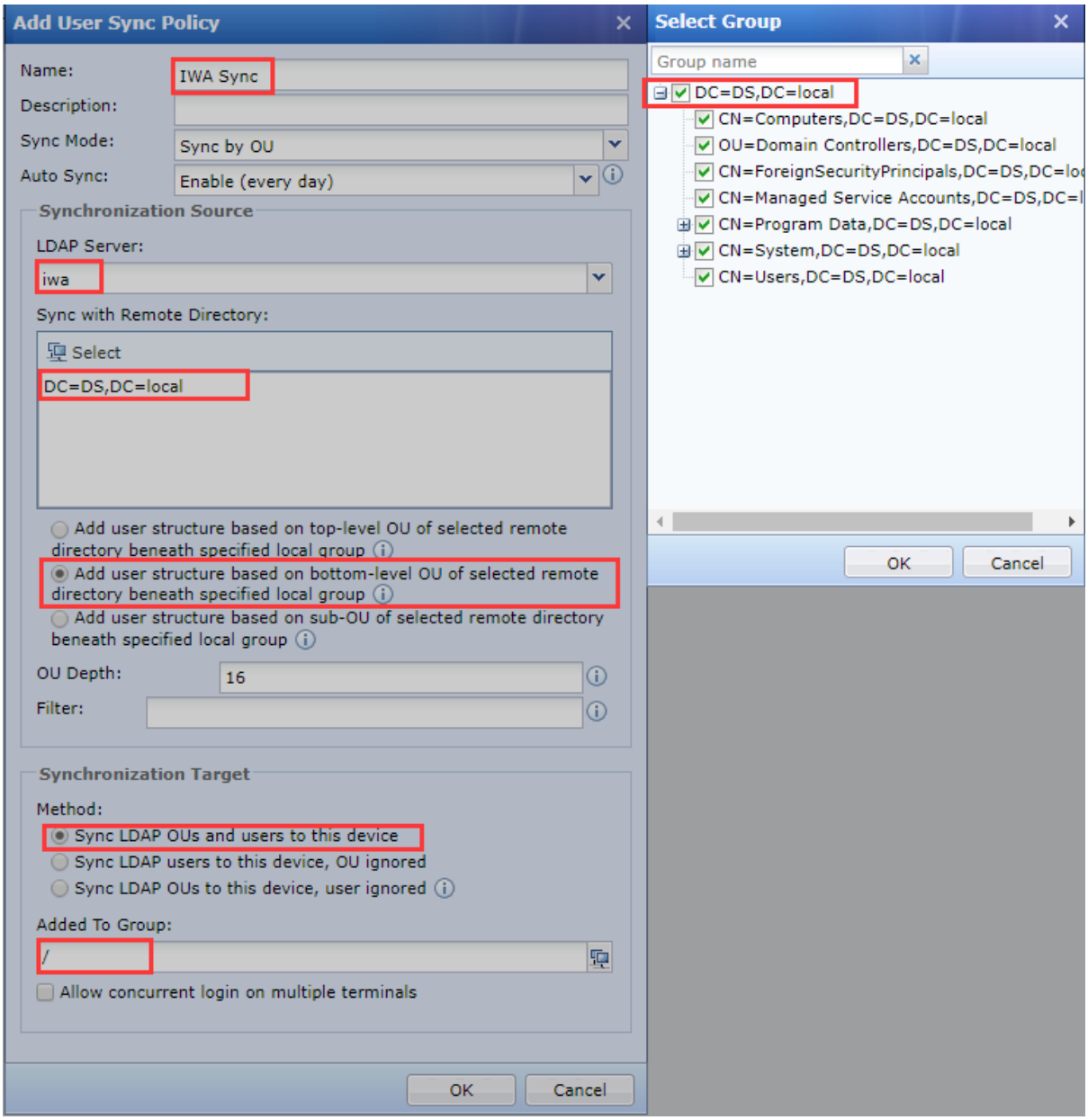

Add LDAP Server
Enable
Name:
iwa
Basic Settings
Address:
192.168.19.177
Port:
389
Timeout(sec):
5
Base DN:
DC=DS,DC=local
Sync Options
Type:
MS Active Directory
Anonymous Login:
Enable anonymous login
Admin DN:
It is used to bind username of server or user DN
admin@DS.local
Password:
User Attributes:
sAMAccountName
Group Attributes:
member
Group:
objectCategory=group
Description Attribute:
description
Search
Paged Search:
Use extension function
Page Size:
0
Size Limit:
0
Test Validity
OK
Cancel


Test Validity
Connect to server and bind with user successfully.
OK

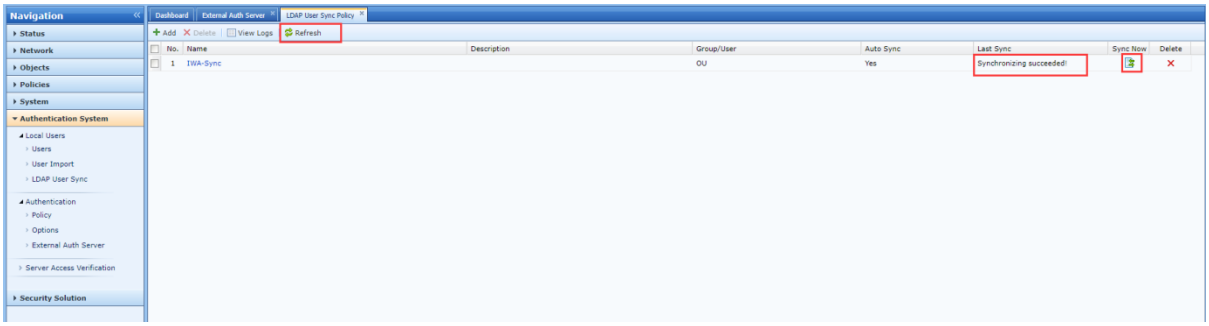
3. In **Authentication System** > **User** > **LDAP User Sync**, click **Add** button and LDAP User Sync policy configuration page will prompt out.

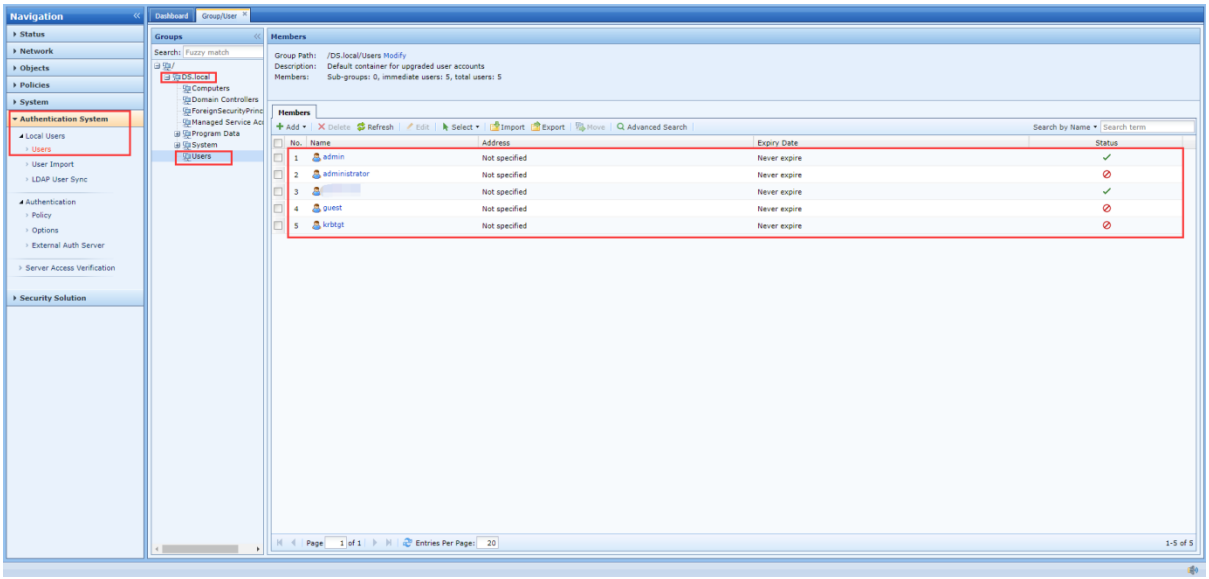


4. Enter the policy name "IWA Sync", select the external authentication server “iwa“ configured just now in the **Synchronization Source** > **LDAP Server**. Select "DC=DS, DC=local“ in the organization structure and click OK. Select "**Sync LDAP OUs and users to this device**" which is the default option for the synchronization target “**Method**“. Select root group “\“ for “**Added to group**“. Click OK.

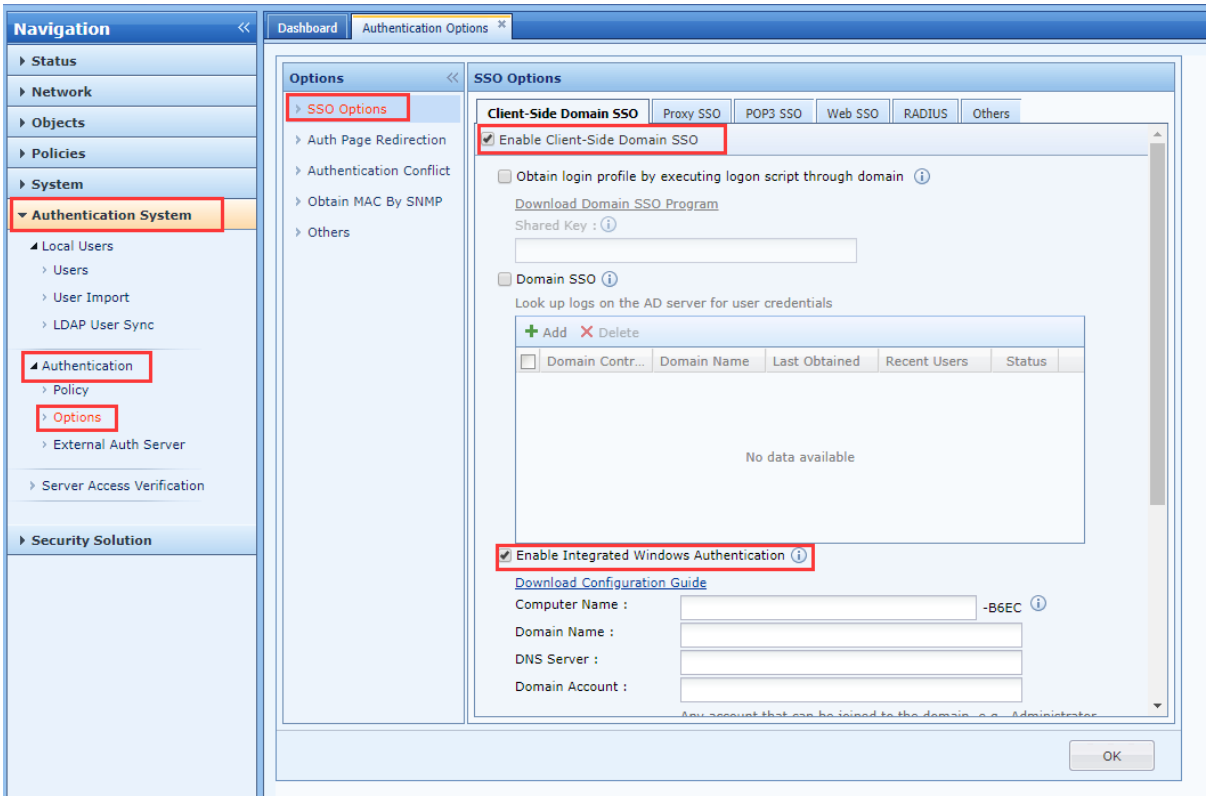


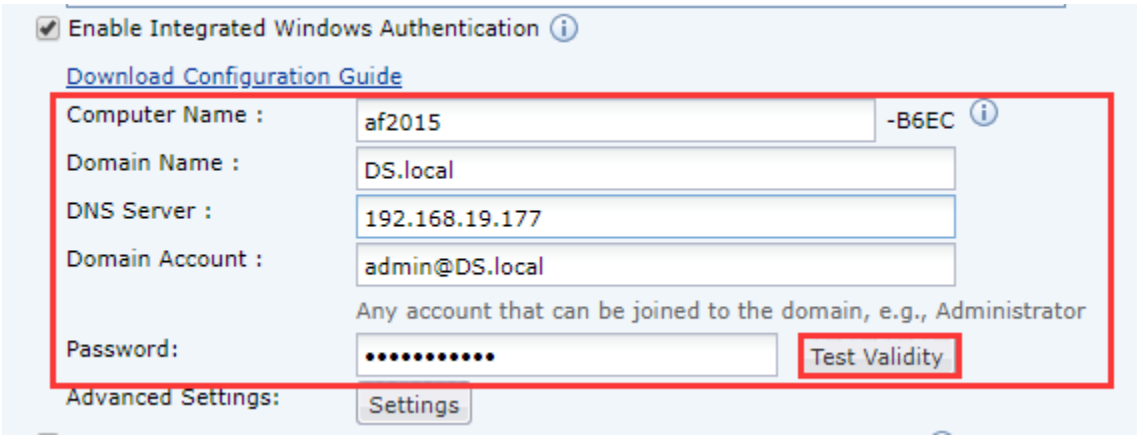
5. Click **Sync Now** button follow by **Refresh** button. The sync status display **Synchronizing Suceeded**. Go to **Authentication System** > **Local Users** > **Users**, the OU and user in domain **DS.local** is successfully imported.

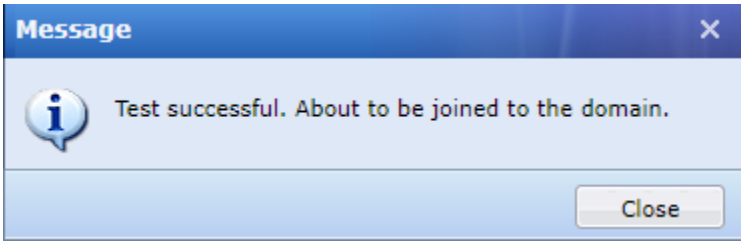




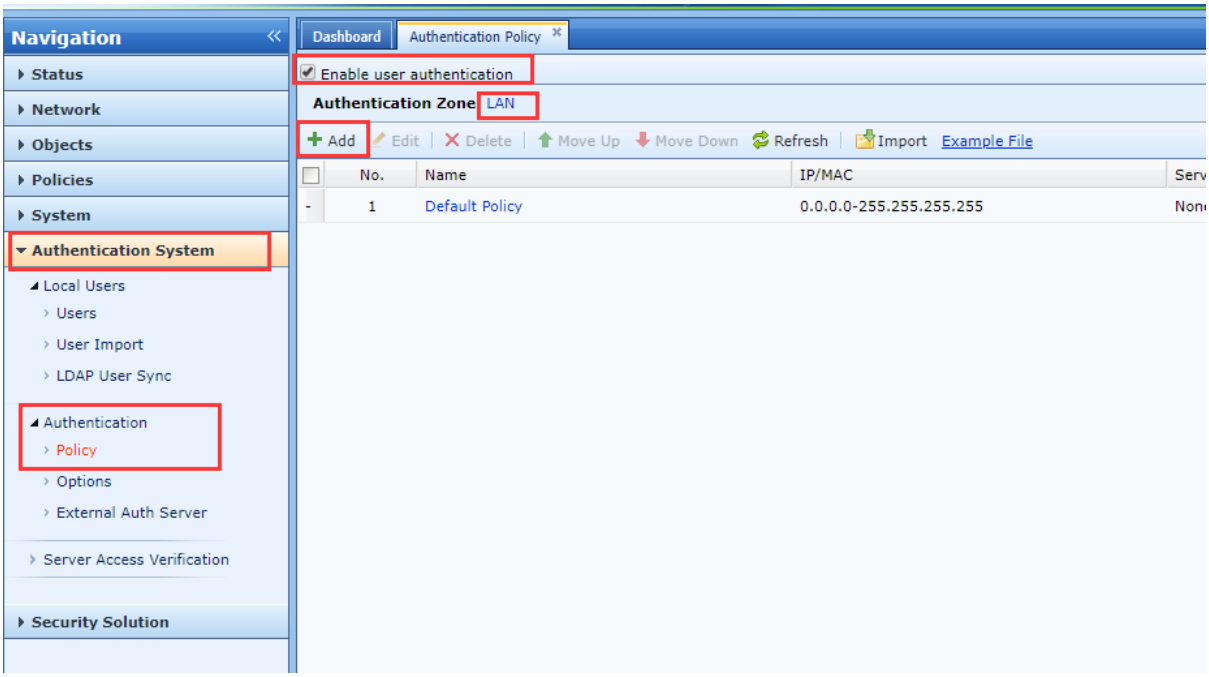
6. In **Authentication System** > **Authentication** > **Options** > **SSO Options** > **Client-Side Domain SSO**, check for the **Enable Client-Side Domain SSO** and check for **Enable Integrated Windows Authentication**. Enter af2015 for Computer Name, DS.local for domain name, 192.168.19.177 for AD dns server. Enter domain account with privilege and corresponding password. Click Test Validity button and prompt "**Test successful.About to be joined to the Domain.**"



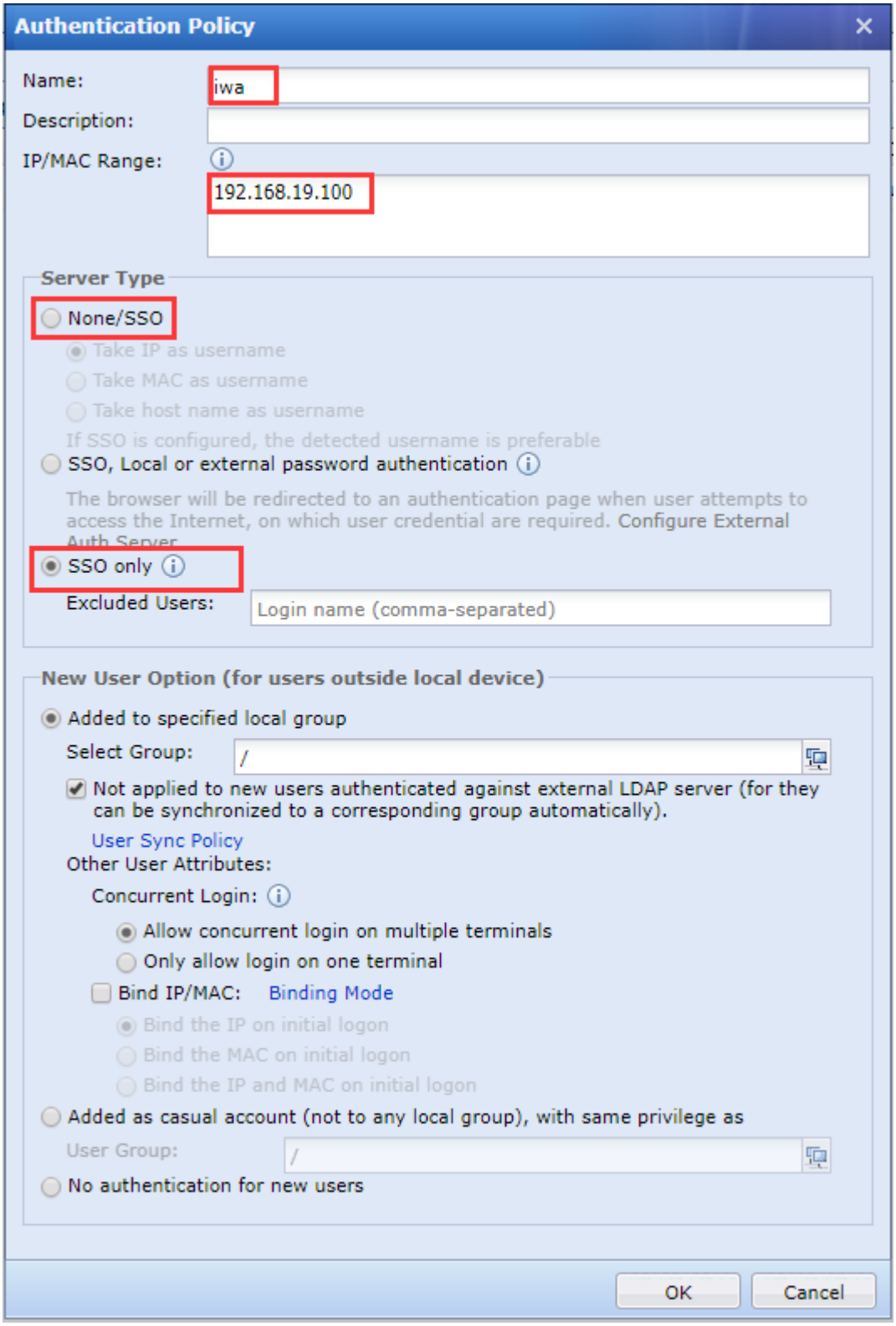




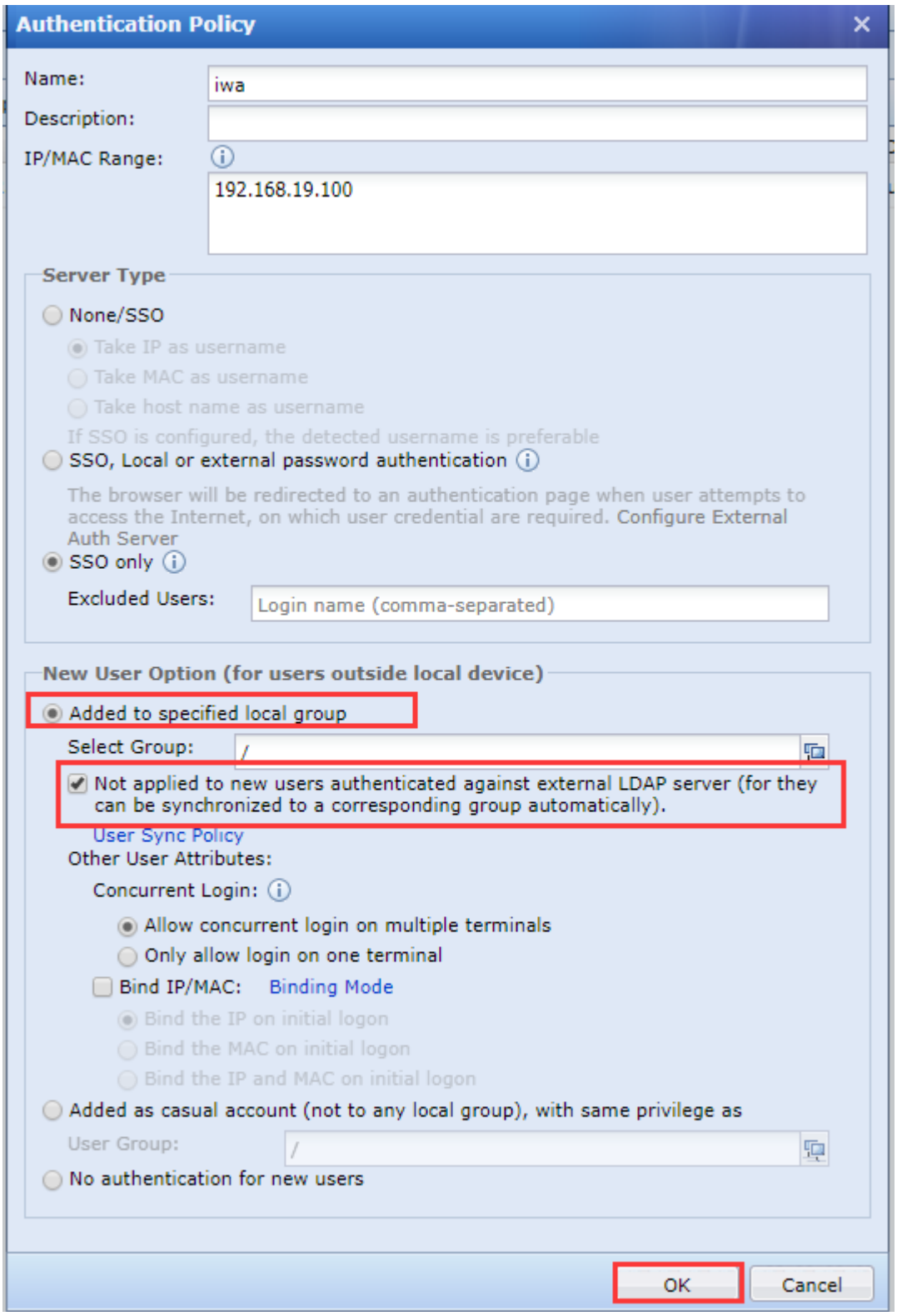
7. In **Authentication System** > **Authentication** > **Policy**, check for **Enable user authentication** and select **LAN zone** which the user located. Click **Add** button and authentication policy configuration page will prompt out.



8. Enter iwa for policy name, 192.168.19.100 for **IP/MAC Range**. For authentication methods, both **None/SSO** or **SSO Only** can be selected. In this testing, **SSO Only** is selected for easier observation.



9. In the new user option of the authentication policy, select **Add to specified local group**, and select "**Not applied to new users authenticated against external LDAP server (for they can be synchronized to a corresponding group automatically)**", then click OK.



Chapter 6 Precautions

1. IWA is not supported in bypass mode.
2. When the device joined domain, will register a DNS record in DNS server with device name and ip 1.1.1.2.
3. The computer joins the domain. In some cases, the domain name suffix is not automatically added. The suffix should be added by default. If the domain name suffix is not added, the ticket submission and iwa will be unsuccessful.
4. IWA supported browser types:
   a. IE-based browser support such as IE, Sogou, 360, Window of the World, etc.
   b. Chrome by default supported
   c. Firefox needs configuration to support.
5. After the device name is added to the domain, the device name is changed to the previous name and added to the domain. At this time, iwa is unsuccessful. You need to restart the computer to log in to the domain and regain the ticket. If the computer is not restarted, since the device name has not changed, the ticket submitted by the computer is still the old one, and the AF device cannot resolve it.