Integrated Windows Authentication Configuration Guide

1 Overview

Integrated Windows Authentication (IWA) is a single sign-on (SSO) solution provided by the Windows system. It allows users who have already logged in to a Windows domain to automatically log in to third-party web apps without re-entering their credentials.

This document describes how to enable and configure IWA on IAG. After configuration, internal PCs that have joined the domain can access the internet through IAG without authentication.

IAG provides two authentication-free mechanisms: NTLM and Kerberos. In proxy internet access scenarios, IAG acts as a proxy server and supports SSO through NTLM. In non-proxy internet access scenarios, Kerberos can be used to complete SSO.

2 Prerequisites

Before configuration, ensure that the following conditions are met.

Resource Type	Requirement	Remarks
AD domain environment	Windows Server with AD domain server is installed. The Windows Server version must be Windows 2000 or later.	For installation instructions, see Install Active Directory Domain Services on Windows Server | Microsoft Learn.
AD domain account	The account type can be one of the following: a) Domain admin account b) Normal user account with permissions to join a server to a domain	For details on how to create a new account, see Domain account does not exist. For permission configuration, see section 3.2 AD Domain Configuration.
	The account must be available: a) The account has not expired. b) The account is not disabled. c) The account password is valid.	
Domain DNS server	IAG can resolve the AD domain name to its IP address. You can use one of the following methods: a) Use the DNS resolution capability built into the AD domain. b) Use an independent DNS server for resolution.	
	The DNS server time must be synced with IAG.	
Network connectivity	IAG can access the LDAP service of the AD domain, and port 389 must be accessible.	
	IAG can access the SMB service of the AD domain. Ensure that the following ports are accessible: a) Port 189 (unencrypted communication) b) Port 445 (encrypted communication; port 189 is unnecessary when encryption is enabled)	
	IAG must communicate properly with the AD domain via port 88.	This port is used by the Kerberos protocol for authentication and ticket requests.
	IAG must communicate properly with the DNS server via port 53.	This port is used by the DNS protocol for resolving domain server IP addresses.

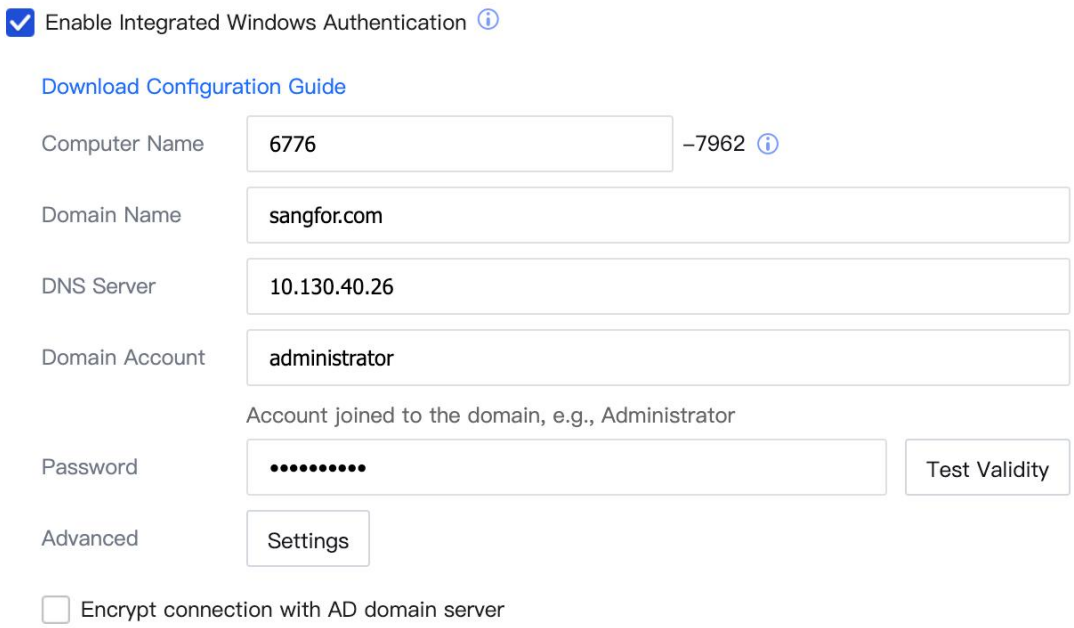
3 Configuration Procedure

3.1 IAG Configuration

3.1.1 Configuration Procedure

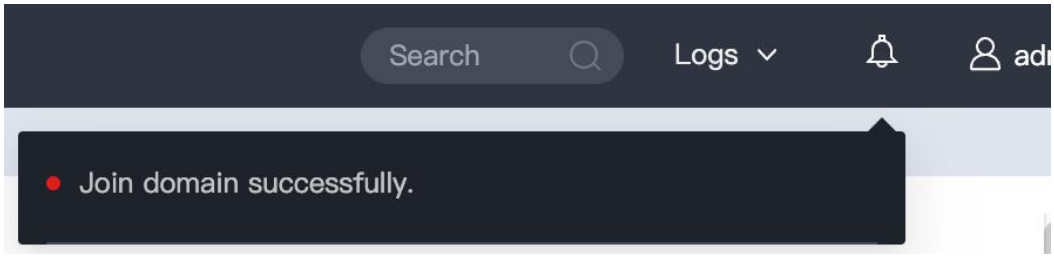
Enable Integrated Windows authentication

- Log in to admin console of Sangfor IAG device;
- Navigate to Access Mgt > Authentication > Web Authentication > Single Sign-On (SSO);
- Click on **MS AD Domain** tab to enter MS AD Domain page;
- Select the options **Enable Domain SSO** and **Enable Integrated Windows authentication**.



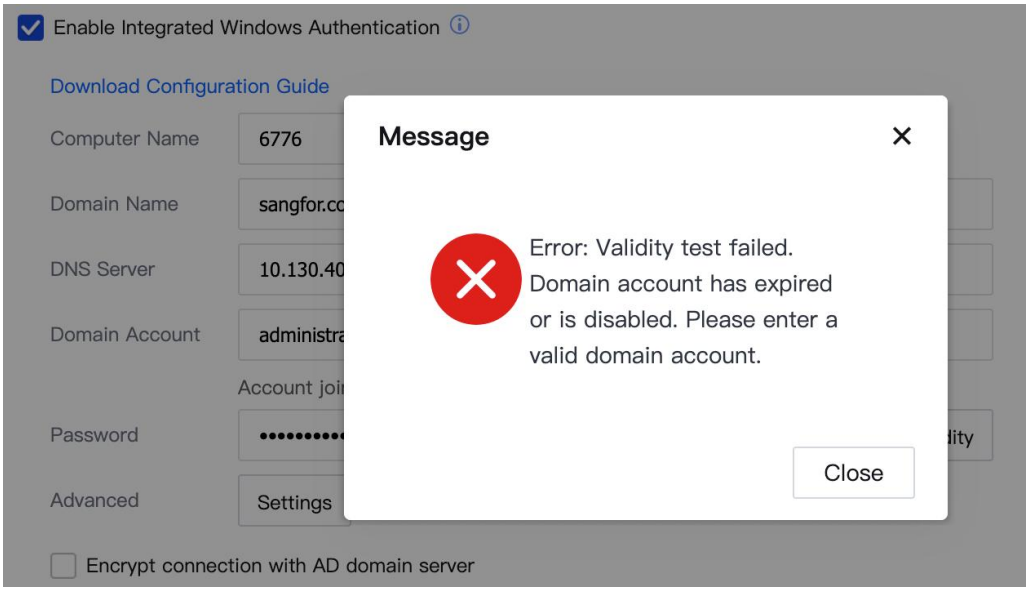
1. Configure Integrated Windows authentication

- Fill in required fields, such as Computer Name, Domain Name, DNS Server, Domain Account and Password.
- Click on **Test Validity** button to test entered parameters. Click Commit to save settings if validity testing succeeds.
- About 10 minutes later, it gives message if the device is joined to the AD domain successfully.

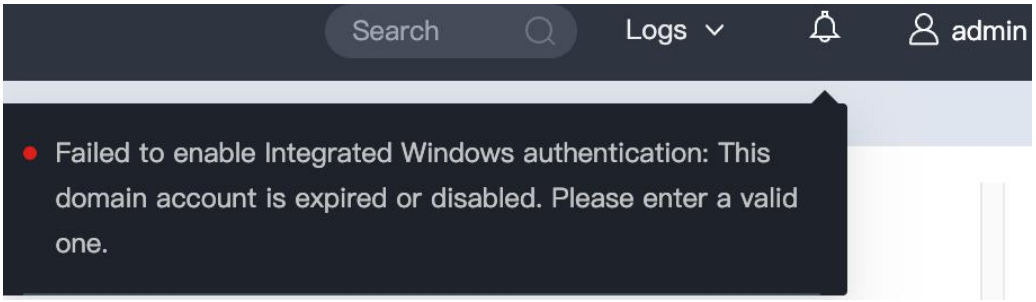


3.1.2 Quick Troubleshooting Guide

- If validity testing fails, a prompt dialog pops up which describes error details.



- If device fails to be joined to AD domain, a prompt message pops up at the right top of this page 10 seconds later, which describes the reason and gives suggestion to administrator.



3.1.3 Parameters

Parameter	Requirement	Length	Description
Computer Name	Letters, digits and hyphen supported only.	At most 10 characters.	Device uses the complete computer name (custom name+"-"+gateway ID) to be joined to AD domain.
Domain Name	Letters, digits, Hyphen and underscore supported only.	Support up to 95 characters	Domain name of the domain to which the device is to be joined.

Parameter	Requirement	Length	Description
			Example: logon2008r2.com
Domain Server	Dotted decimal supported only, for example, 192.168.222.132	One IP address allowed only	IP address of DNS server. DNS server and domain controller often reside on one computer, but can also be on different computers.
Domain Account	Chinese characters , space and special characters (”’% \) not supported.	Support up to 95 characters.	Both administrator account and non-administrator account supported. The domain account is created on domain controller.
Password	None	Support up to 95 characters.	The password of the corresponding domain account.

3.2 AD Domain Configuration

Windows 2000 and later versions of Windows Server support IWA, including Kerberos and NTLM protocols.

The core principle of IWA is that IAG must join the domain as a computer, and the AD domain must provide an account with sufficient permissions for domain joining. The provided domain account can be either a standard domain account or a domain admin account.

Notice: Microsoft considers NTLM an insecure protocol. Windows Server 2025 has removed NTLMv1 authentication. Although NTLMv2 authentication is still available, Microsoft has announced plans to remove NTLMv2 authentication in future releases.

3.2.1 Join Domain With a Standard Domain Account (Recommended)

A standard domain account has lower privileges, making it easier to meet enterprise requirements for domain account privilege control. It is therefore recommended to use a standard domain account for domain joining.

There are two configuration methods for joining the domain with a standard account: 1. Add the domain account to the Group Policy setting **Add workstations to domain**. 2. Grant the domain account permission to create and delete computer objects. Either method can be used. The differences are as follows.

Domain Join Method	Notes	Summary
Configure group	● IAG joins the domain under the default Computers	It is recommended to

policy	container in AD domain. ● Due to AD restrictions, a domain account can create up to 10 computer objects, meaning the same account cannot be used to join more than 10 devices.	use the method of granting the domain account permission to create and delete computer objects.
Configure computer object create/delete permissions	1. IAG joins the domain under the administrator-specified container (OU). 2. There is no limit on the number of computer objects created, allowing the same domain account to be used on multiple devices simultaneously.	

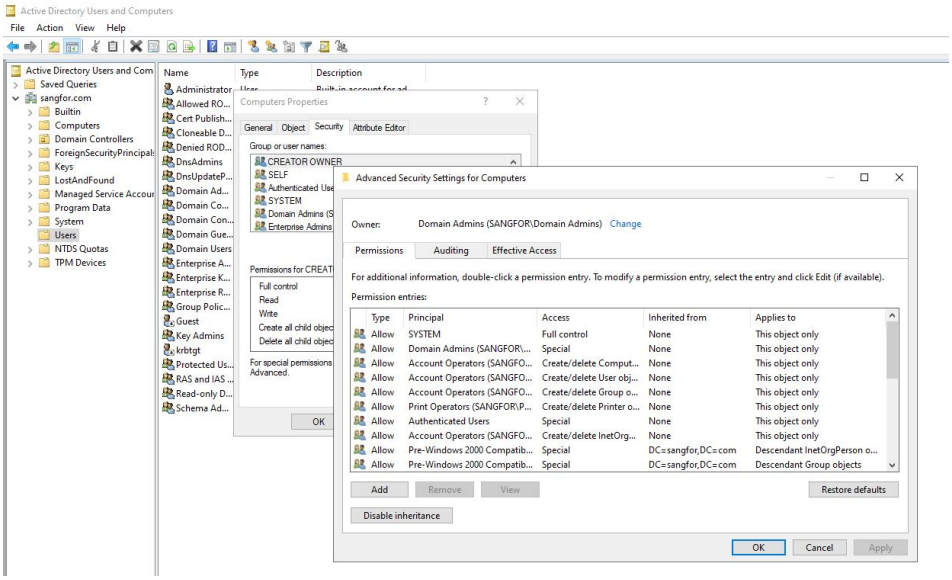
Grant Computer Object Create/Delete Permissions to Domain Account (Recommended)

This method mainly involves two permissions related to computer objects. The details are as follows.

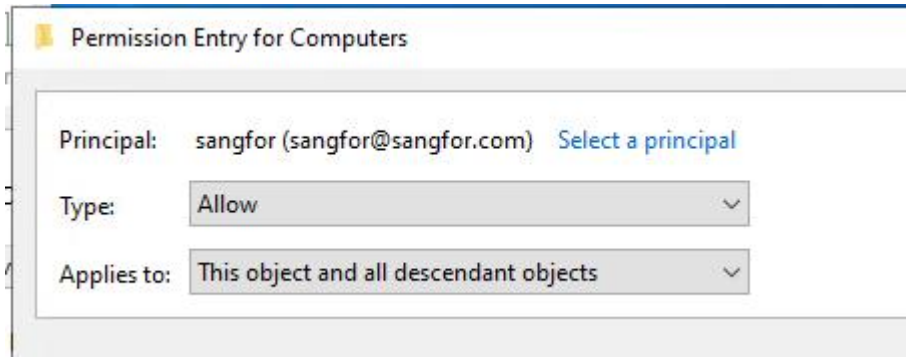
Permission	Object	Permission Scope	Remarks
Create Computer objects	AD domain root node or Computers container	This object and all descendant objects	Required. Used to create a computer object with the specified computer name in the Computers container and associate it with IAG.
Delete Computer objects			Optional. Used to delete the computer object created during domain joining when IAG leaves the domain. If not selected, the object must be manually deleted to avoid residual data affecting future domain joining.

Configuration procedure:

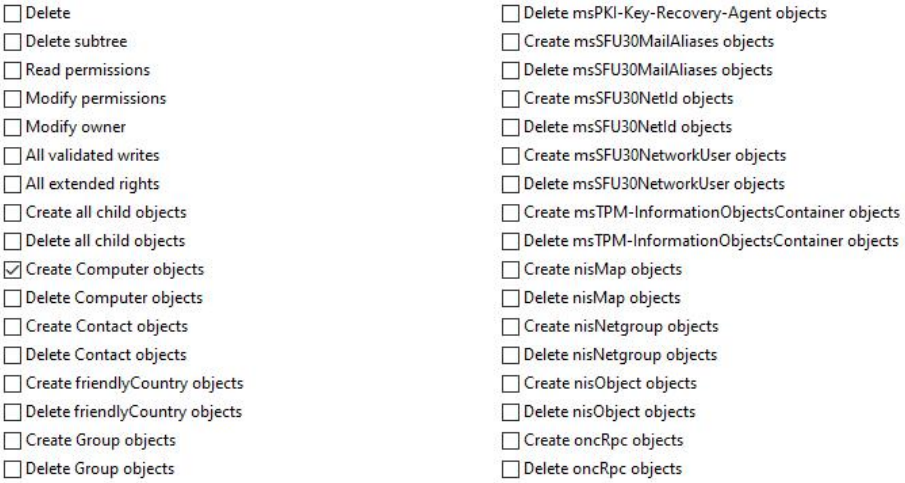
Go to **Active Directory Users and Computers**, right-click the domain root node or **Computers**, and select **Properties** to view the properties of the domain root node or Computers container. Click the **Security** tab and click **Advanced**. In the pop-up window that appears, click the **Permissions** tab and click **Add**.



In the **Permission Entry for Computers** pop-up window, click **Select a principal** in the **Principal** field, select the domain user to grant permissions to, set **Type** to **Allow**, and set **Applies to** to **This object and all descendant objects**.



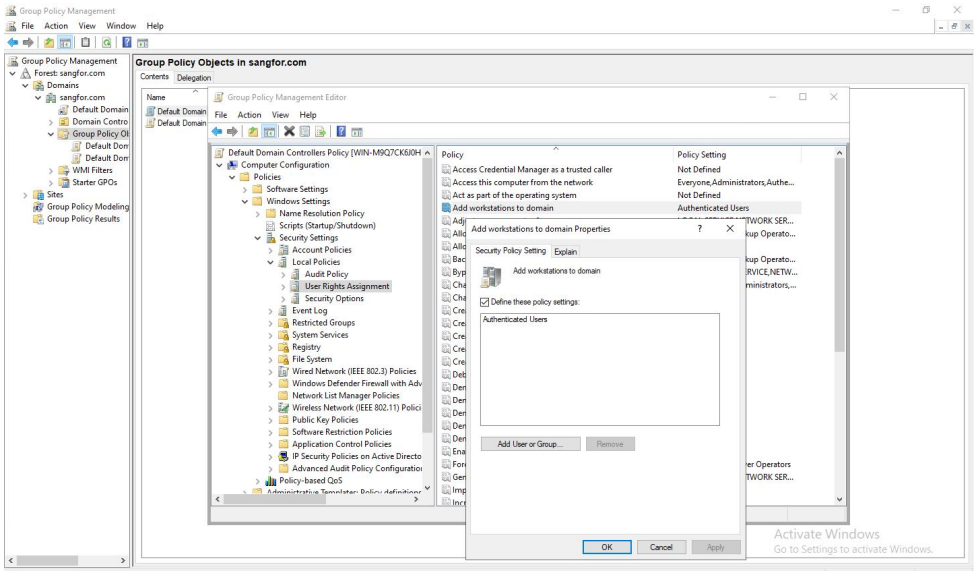
In the permission list, select at least **Create Computer objects**.



Add the Domain Account to the Group Policy Setting "Add Workstations to Domain"

Go to **Group Policy Management** > **Group Policy Objects** > **Group Policy Management Editor**. In the **Group Policy Management Editor** pop-up window, choose

Computer Configuration > **Policies** > **Windows Settings** > **Security Settings** > **Local Policies** > **User Rights Assignment**, and click **Add workstations to domain**. In the **Add workstations to domain Properties** pop-up window, click the **Security Policy Setting** tab, and add **Authenticated Users** or the specified domain join account.



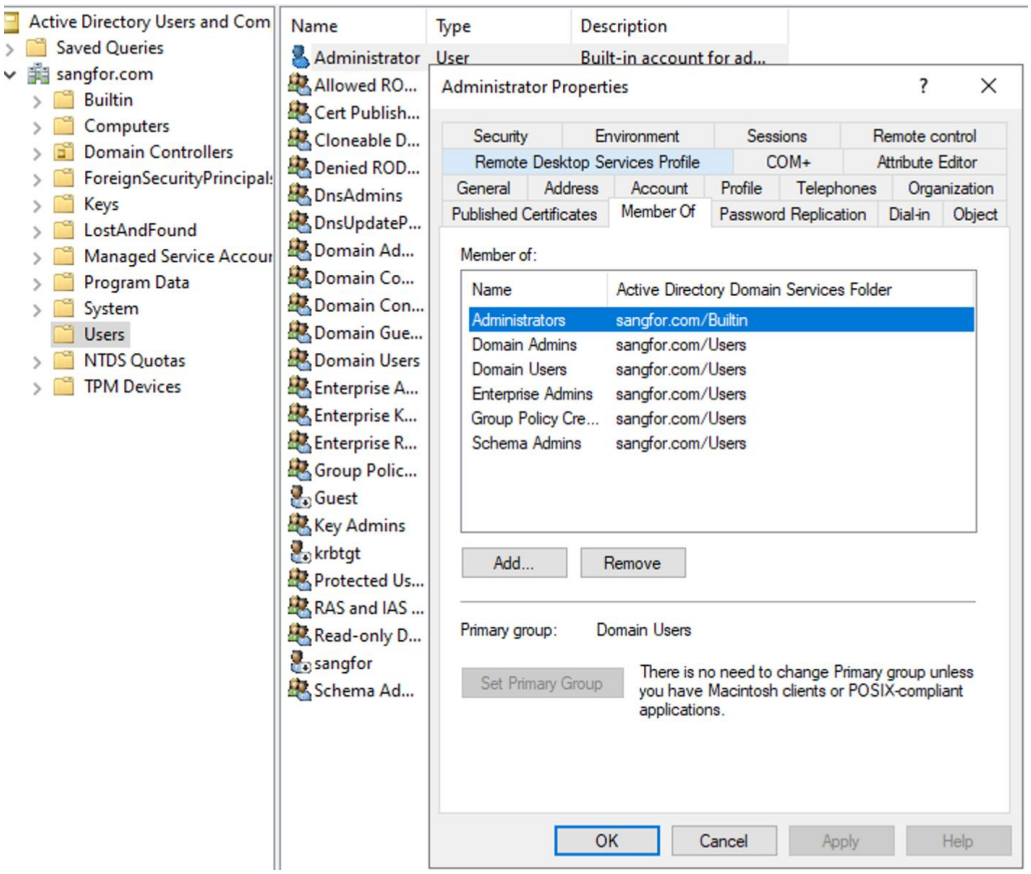
3.2.2 Join Domain With a Domain Admin Account

Permissions are based on the user's group membership. This account can create computer objects in any OU without quantity limits and has full control over the created objects.

The management account must be a member of the Domain Admins security group. This account has high privilege, so this method is not recommended for enterprises with strict domain privilege control. Method 1 is preferred in such cases.

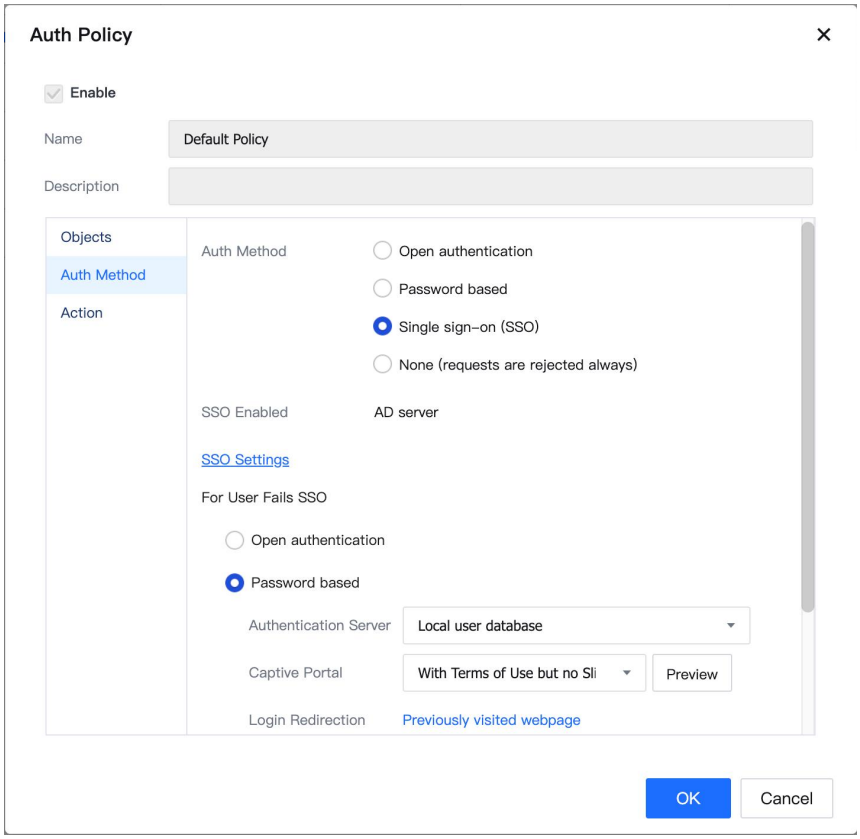
AD Domain Configuration Procedure

Go to **Server Manager** > **Dashboard**, open **Active Directory Users and Computers** pop-up window, view the properties of the domain join account, and add the **Domain Admins** security group on the **Member Of** tab.



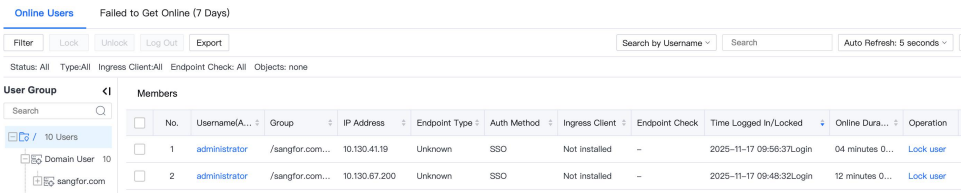
4 Scenario: Domain SSO

1. Navigate to **Access Mgt > Authentication > Web Authentication > Authentication Policy**, edit default policy and select **Password Based** or **Single Sign-On (SSO)** as **Auth Method**. Then click **Commit** to save the changes.



2. Log in to PC with your domain account and access Internet using browser. If Internet access is successful, go on the next step.

3. Log in to admin console of IAG unit. Go to **Status > Users > Online Users** page and check if that domain account exists among online users and the **Auth Method** is SSO. If that entry exists, it indicates that Integrated Windows authentication works.



5 FAQ

5.1 Possible Error Messages

1. Unable to connect to DNS server

Solution:

Check if the network connection between device and DNS server is OK.

2. Unable to find the domain on DNS server

Solution:

Check if the domain name is correct. If it is incorrect, provide a valid one.

3. Unable to connect to domain controller

Solution:

Check if the network connection between device and domain controller is OK.

4. Invalid domain name

Solution:

Make sure the domain name you entered is valid, not a computer name or other non-domain name. If it does not work, contact network administrator to check if the domain controller works improperly.

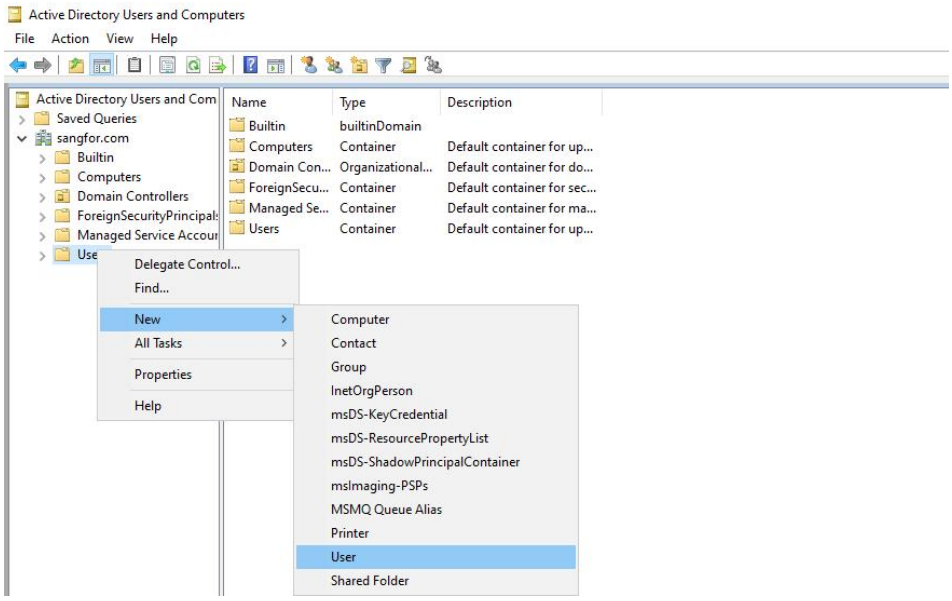
5. Domain account does not exist

Solution:

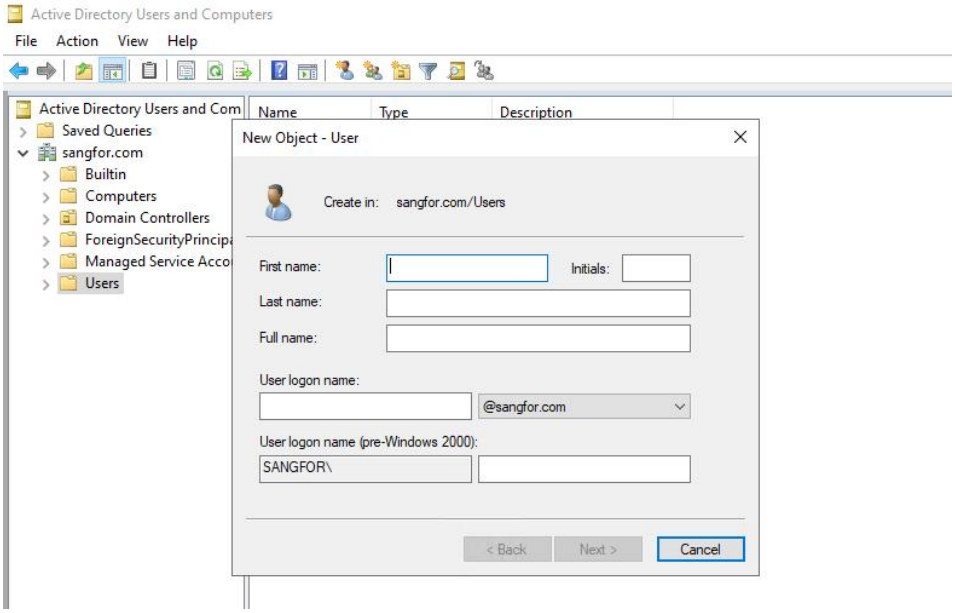
Re-type a valid domain account or create a new one on AD domain, then type the newly-created domain account.

Instructions on how to create AD domain user account:

- Right-click on **Users** group and Select **New > User**.



Type user logon name, click **Next** and type password. Finally, click **Finish** to save changes.



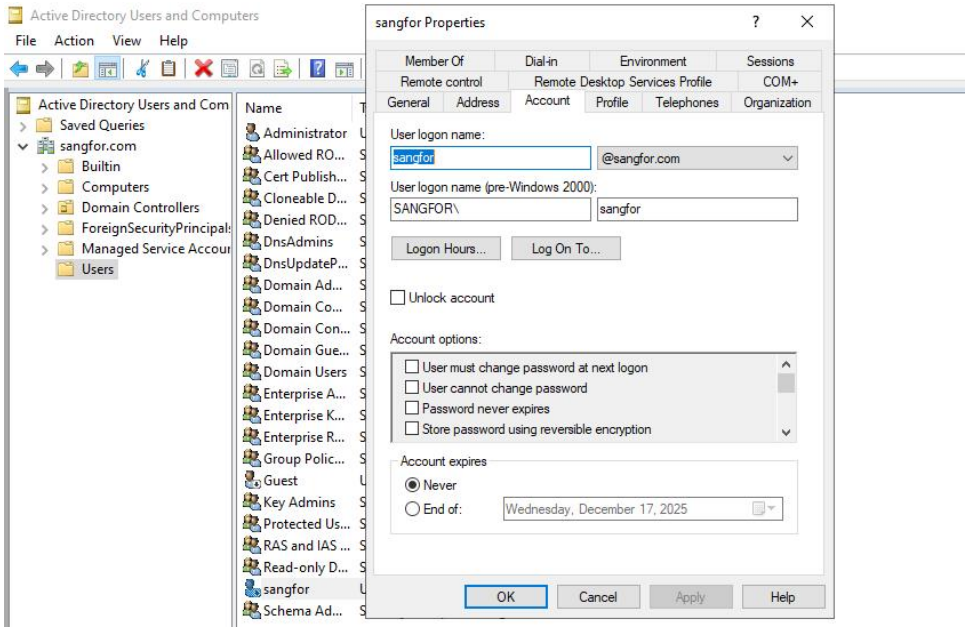
6. Domain account is expired or disabled

Solution:

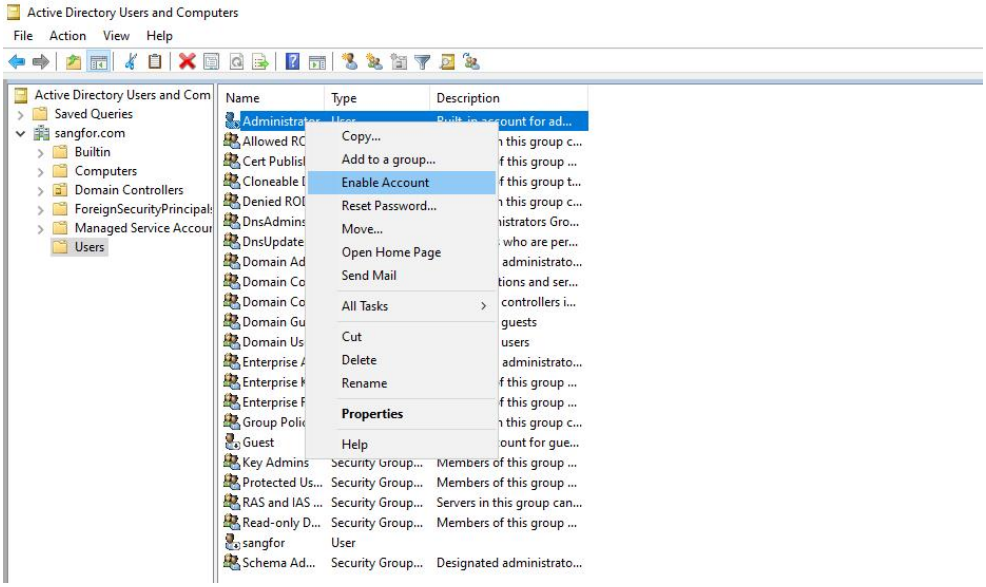
Contact network administrator to check if the domain account gets expired; if it is expired, change expiry date of that account; if it does not expire, it indicates it is disabled, then you can make this account valid simply by enabling it again; or use another domain account to have device joined to AD domain.

Note:

- Change expiry date. Log in to AD domain, select the domain account to enter its properties page and click **Account** to enter **Account** tab. In **Account options**, select **Never** or **End of** to set a new expiry date again.



- Right-click on that domain account in **Users** group and select **Enable Account** to enable this domain account.



7. Password of domain account is incorrect

Solution:

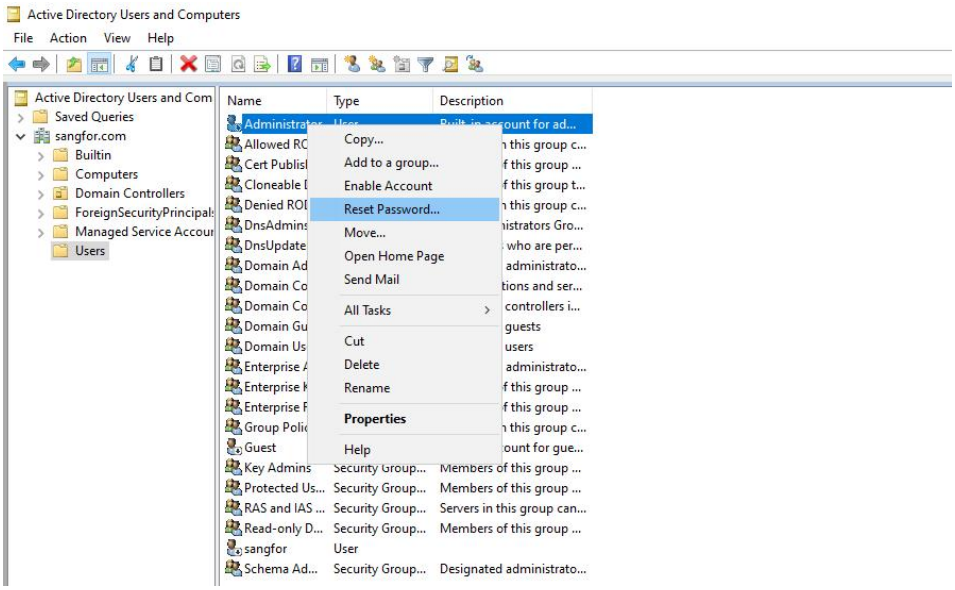
Retype a correct password.

8. Password of domain account is expired

Solution:

Use another domain account or contact network administrator to reset the password of that domain account.

Note: To reset domain account password, log in to AD domain and right-click on that domain account, and select **Reset Password** to reset password.



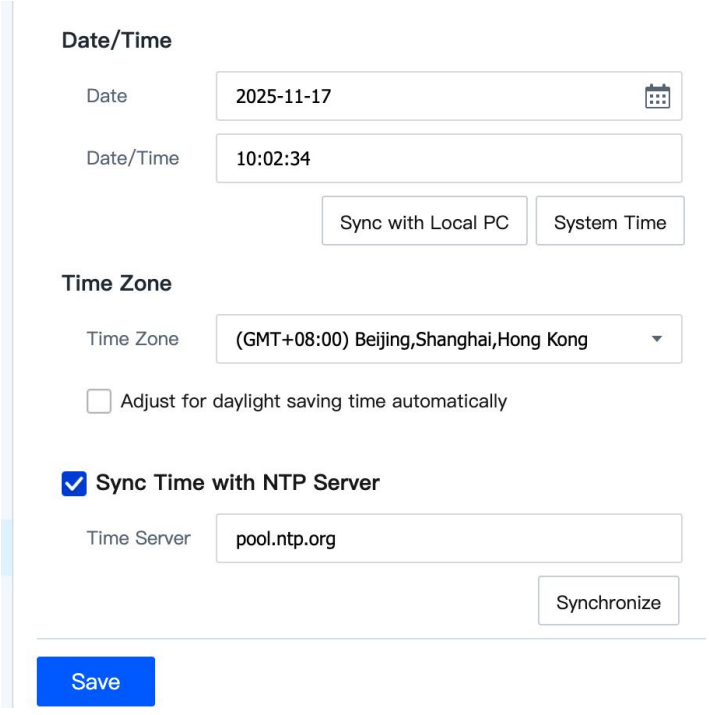
9. System time is inconsistent with that on domain controller

Solution:

Log in to admin console of IAG unit to check if system time and time zone are inconsistent. If they are inconsistent, change them on either the IAG unit or domain controller to make them consistent.

Note:

- Go to System > General > Date/Time and click System Time to obtain system time.



- Modify system time and time zone. To apply changes, click **Commit**.

10. Privilege of this domain account is insufficient

Solution:

Refer to the AD Domain Configuration section to check whether the permission settings are correct.

Change computer name or domain account to the administrator account.

11. The domain account has been used too many times to join computers into the domain

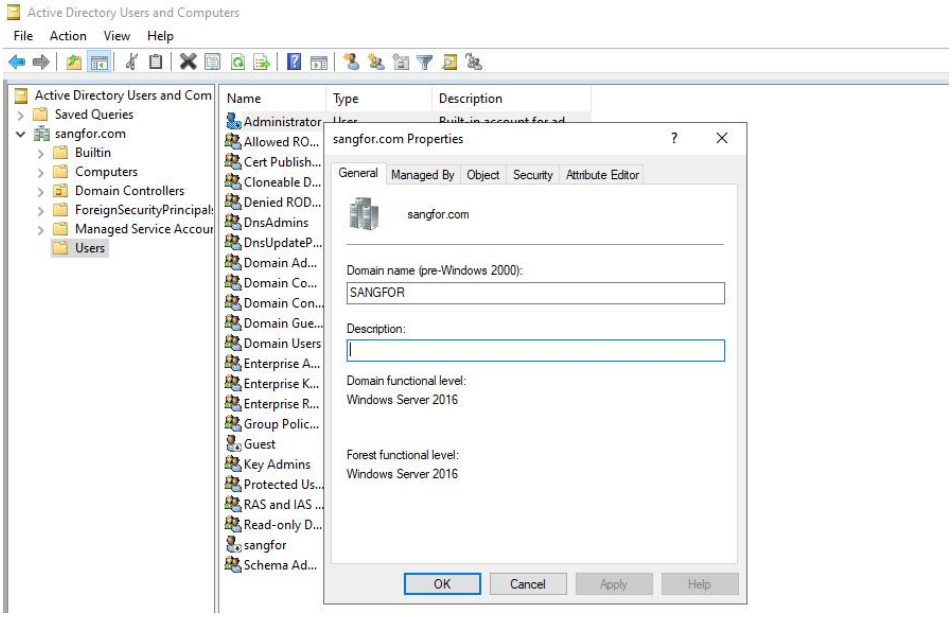
Solution:

Use another domain account.

12. Domain name for Windows 2000 earlier version is incorrect

Solution:

Enter the domain name in **Advanced > Settings** on the **MS AD Domain** page. You can obtain the domain short name from the properties of the domain root node.



13. Failed to register on DNS server

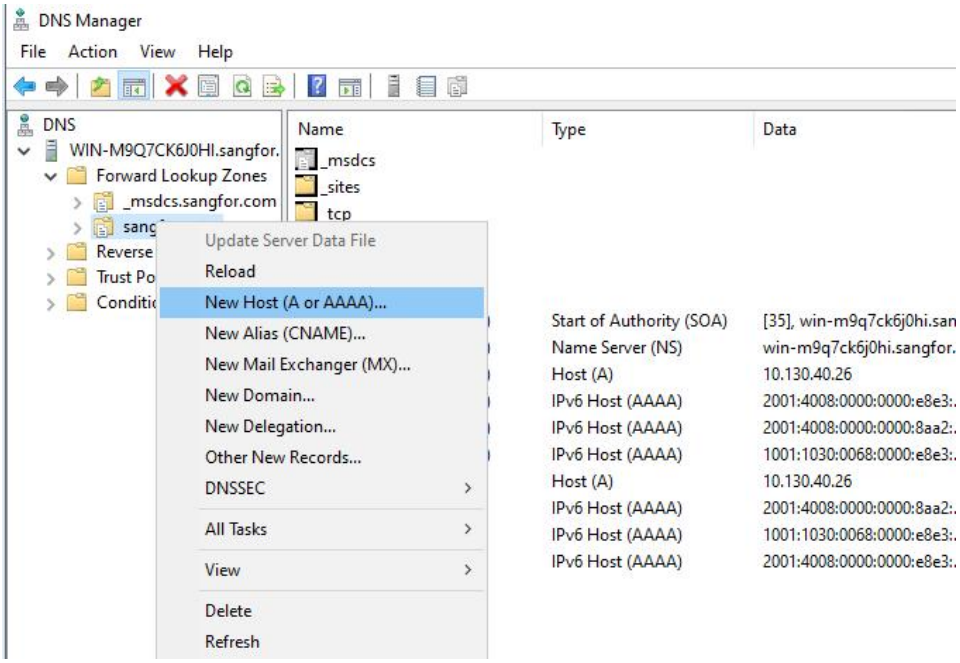
Solution:

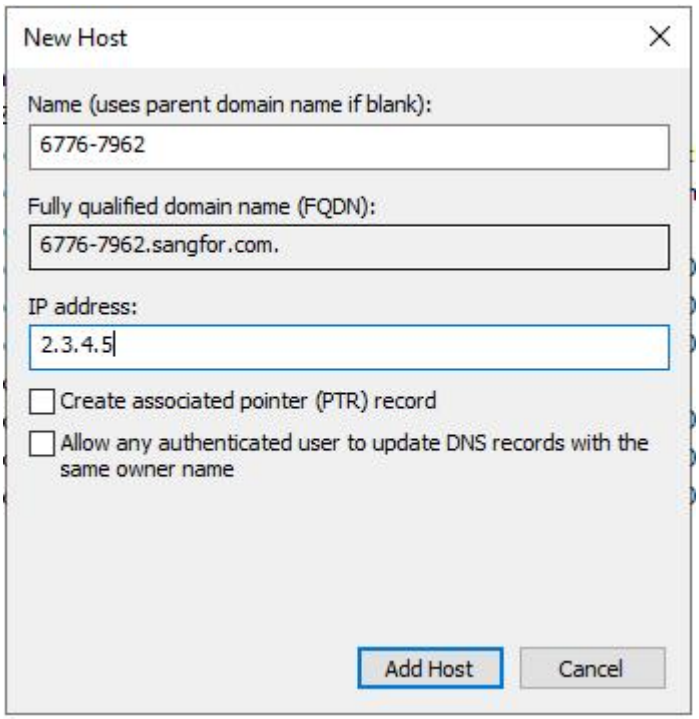
1) Check if system time is consistent with that on DNS server; if they are inconsistent, click Sync with Local PC to synchronize time with DNS server.

2) If registering device fails again, add this device entry on DNS server.

Instruction on how to add device entry on DNS server:

On DNS server, create new host. On the **New Host** page, enter computer name (custom name + '-'+ gateway ID) and the IP address of IAG unit (default 2.3.4.5, or enter the IP address configured on IAG or another reachable virtual IP address). Click **Add Host** to complete adding new host.





14. Failed to join parent or child domain

Solution:

(1) IAG device can only join either the parent or child domain. To join the child domain, exit the parent domain first, and vice versa.

(2) Refer to section 3.2 AD Domain Configuration to add the required domain join permissions.

(3) Check whether the domain name resolution is correct.

5.2 Other Errors

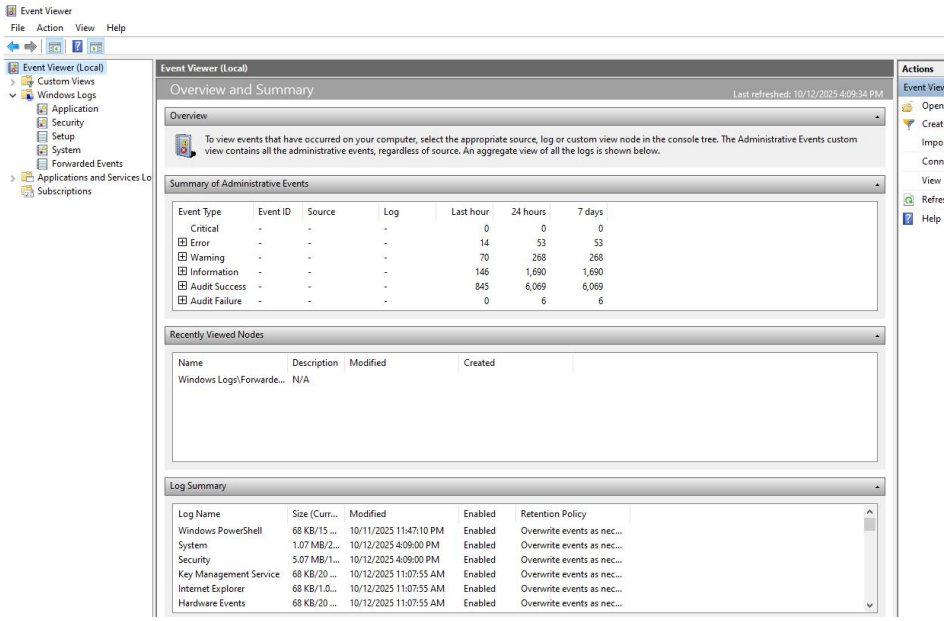
Failed to join domain

The cause of this error is unclear and may differ based on the context. Try the following methods:

(1) Refer to section 3.2 AD Domain Configuration to check permission settings.

(2) Use an administrator account to join the domain.

(3) Check the server event logs.



If the problem persists, please call +60 12711 7129 (7511).

5.3 Notes

1. After the device successfully joins the domain, the authentication service will restart for about 5 seconds, during which users cannot authenticate.

2. Once the device is joined to domain, it will not be joined to that domain again in case that no change is made to relevant settings, though you click **Commit** repeatedly

Appendix

1. Kerberos Authentication Principle

1. The client initiates an initial request.

2. IAG (web server) responds with a 401 challenge.

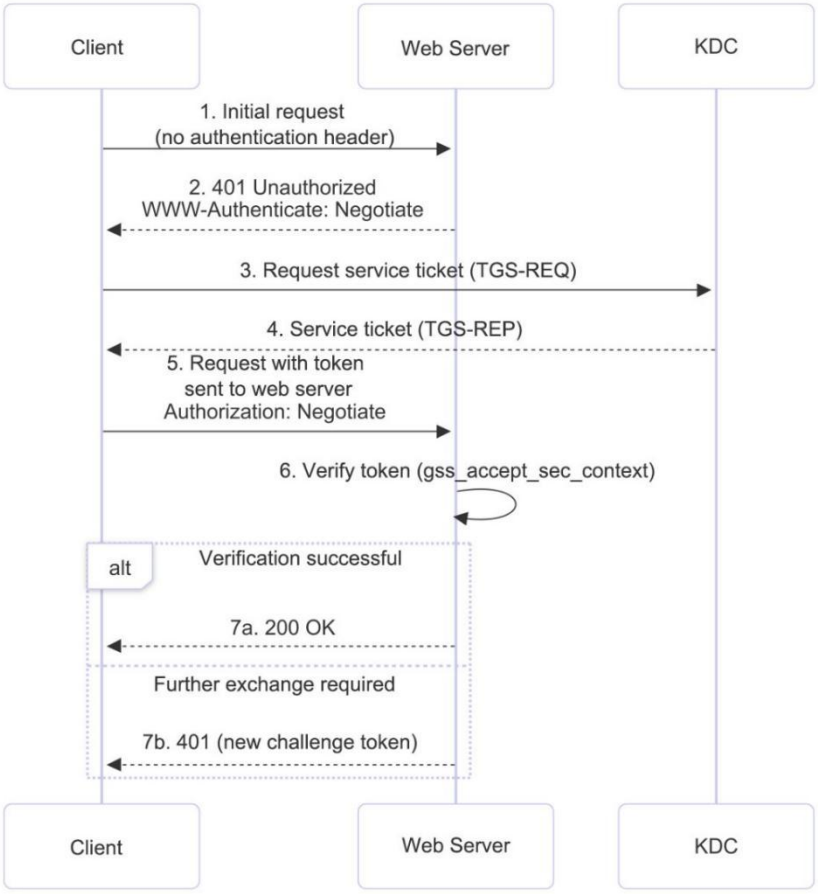
3. The client requests a Kerberos ticket from the KDC (Key Distribution Center, i.e., domain controller).

4. The KDC returns the Kerberos ticket.

5. The client sends an authentication request with the ticket.

6. IAG uses the key generated during domain joining to verify the ticket.

7. If the ticket is valid, IAG responds with a 200 status code, allowing subsequent client requests. Otherwise, it responds with a 401 status code to prompt further authentication.



2. NTLM Authentication Principle

1. The client sends a request to IAG (proxy server).

2. IAG responds with 407, requesting NTLM authentication.

3. The client resends the request with the initial NTLM negotiation message.

4. IAG responds with 407, including the challenge message.

5. The client sends the request with the final authentication message.

6. IAG forwards the authentication message to the domain controller.

7. The domain controller returns the authentication result.

8. If authentication succeeds, IAG responds with 200 status code and allows subsequent proxy requests. Otherwise, it responds with a 407 status code, requiring further authentication.