



**SANGFOR**

# IAM

## IWA SSO Configuration Guide

**Version 12.0.42**

---

## Change Log

Date	Change Description
April 27, 2020	Version 12.0.42 document release.

---

# CONTENT

Chapter 1 Problem Background.....	1
Chapter 2 Solution.....	1
2.1 IWA SSO Authentication.....	1
Chapter 3 Test Environment.....	1
3.1 Topology.....	1
Chapter 4 Configuration.....	2
Chapter 5 Testing Result.....	11
Chapter 6 Precautions.....	11
Chapter 7 Appendix A: LDAPS Configuration Guide.....	13
7.1 Background.....	13
7.2 Configuration of Server Certificate Installation.....	13
7.3 Configuration of LDAPS Server Signing.....	21
7.4 AD Configuration on IAM.....	23
7.4.1 Authentication Port Description.....	24
7.4.2 Enable Encryption.....	24
7.5 IWA SSO Configuration.....	25

# Chapter 1 Problem Background

Customer's environment has AD domain to manage internal users and the IT manager wish to deploy a Sangfor IAM in their network for user authentication purpose. The manager wish to synchronize IAM with their AD controller (Domain SSO) which the process is transparent for internal users so that users do not need to reinsert the log in details again for IAM authentication. Below are some details of customer's requirements:

1. The manager hope to view users online with their user name in AD controller, then audit all the network behavior accordingly to the user name.
2. The manager does not want to change their domain GPO and therefore not allow domain SSO script mode (script mode required to add logon.exe and logoff.exe to the domain) which not comply with their company security policy.

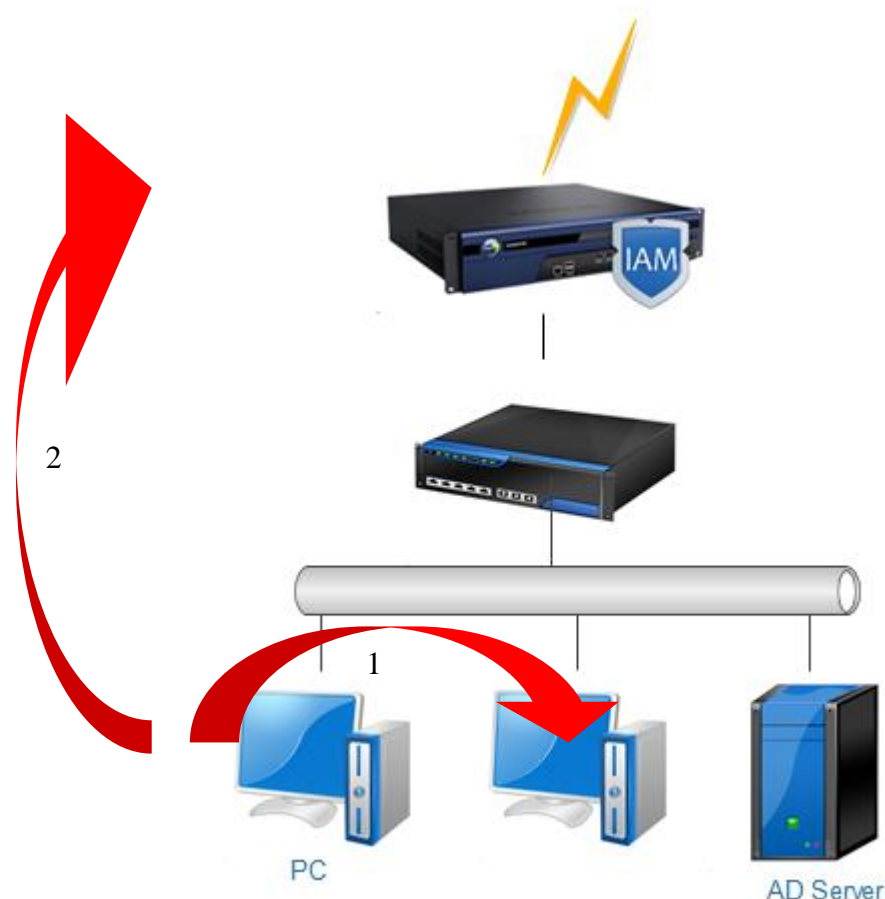
# Chapter 2 Solution

## 2.1 IWA SSO Authentication

In this method, Sangfor IAM will join into customer's windows domain and act as a resource in the domain. When domain PC log on to the domain and browse a website, the request will be halt by IAM and redirect to IAM's resource page. This action will trigger kerberos authentication and IAM will obtain the ticket submit by domain PC then get the details for IWA SSO authentication. However this process is transparent for users.

# Chapter 3 Test Environment

## 3.1 Topology



① PC log on to the domain.

② User browse a website (The processes include domain PC redirect to visit Sangfor IAM resource, trigger kerberos authentication, domain SSO authentication and all process are transparent for end users).

Note: If server signing requirement is enabled on the AD domain, encrypt connection needs to be enabled at the IWA single sign-on configuration, otherwise IWA single sign-on will be affected. [See Appendix B]

## Chapter 4 Configuration

The configuration in IAM basically included 3 steps : add new LDAP server, add new authentication policy and configure IWA domain SSO, as shown below:

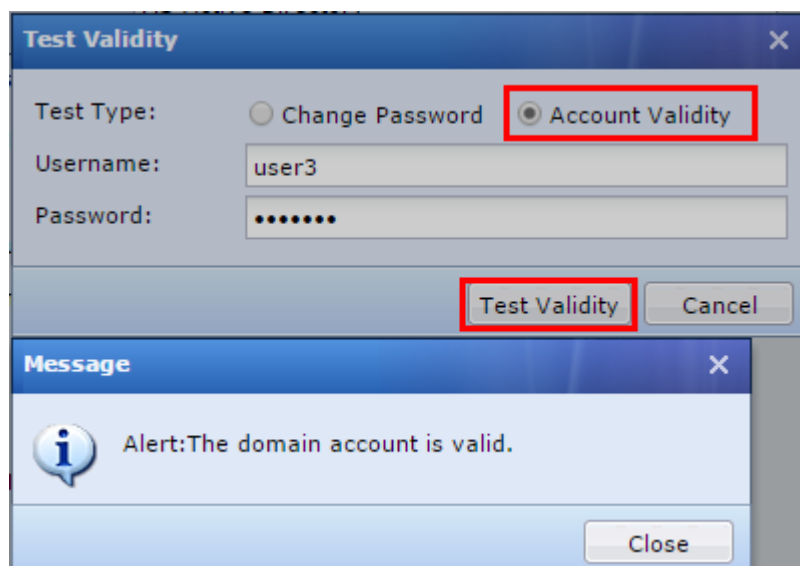
1. Add a new LDAP server.



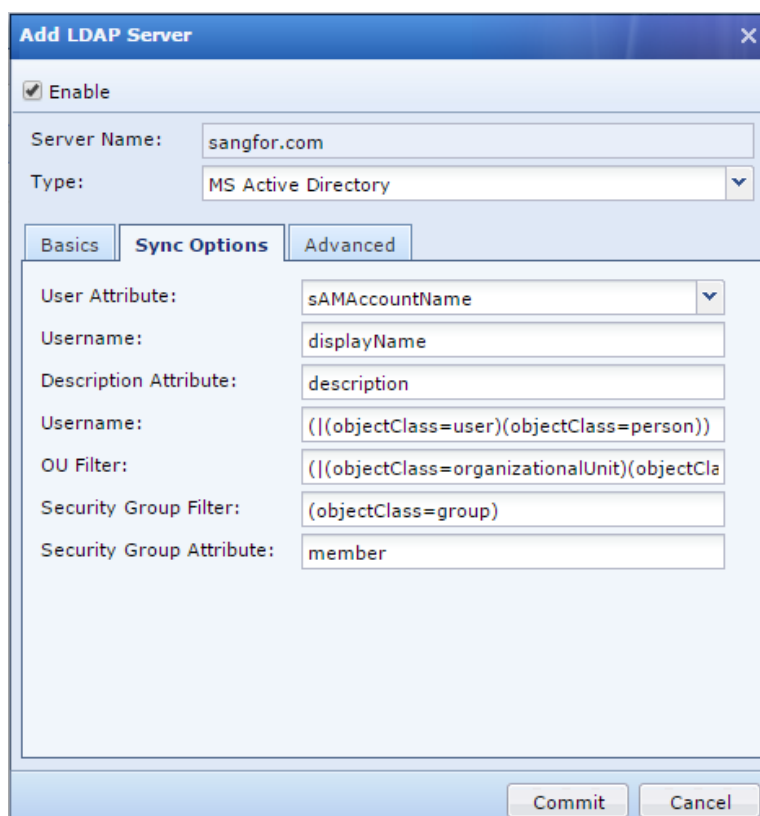
The 'Add LDAP Server' dialog box is shown with the 'Basics' tab selected. The 'Enable' checkbox is checked. The 'Server Name' is '192.168.20.88' and the 'Type' is 'MS Active Directory'. The 'IP Address' is '192.168.20.89', 'Port' is '389', and 'Timeout (sec)' is '5'. The 'Search' checkbox is unchecked, and 'Admin DN' is 'administrator@sccorp.local'. The 'Admin Password' is masked with dots. The 'Enable encryption' checkbox is checked, and the 'Encryption Method' is set to 'TLS'. The 'Verify certificate' checkbox is unchecked. The 'Domain Name' is empty, and the 'Certificate' is '\*.cer'. The 'BaseDN' is 'DC=SCCORP,DC=local'. There is a 'Test Validity' button at the bottom of the 'Basics' tab. At the bottom of the dialog are 'Commit' and 'Cancel' buttons.

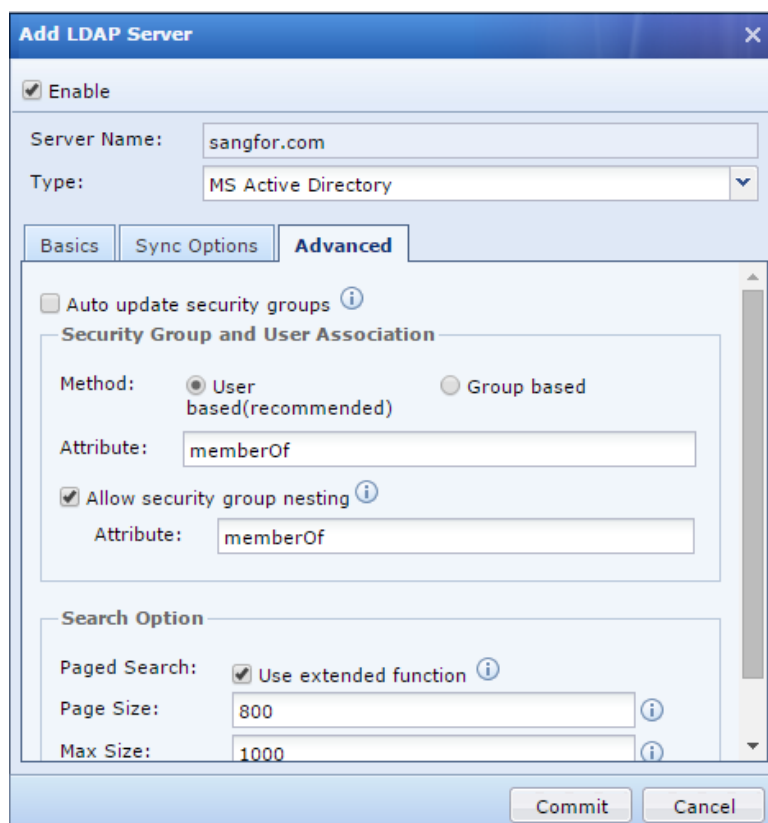
**[Note]**

- The page “**Add LDAP Server**” has an option “**Test Validity**”, it can test domain account validity and change domain account password via this function.

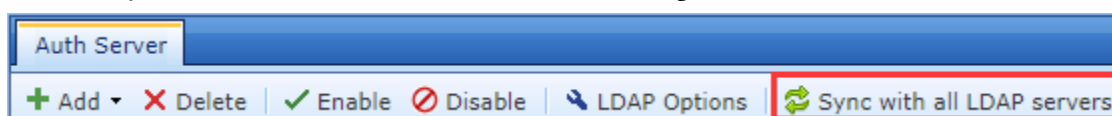


- b) Other than that, the page “Add LDAP Server” contains also “Sync Options” and “Advanced” two tabs, AD domain and SUN domain need only “Basics” configuration, “Sync Options” and “Advanced” configuration keep to default settings. If other domains unable to grab domain OU by using default settings, can fine tune the “Sync Options” to solve the problem. The tabs are shown in the figures below:





- c) If customer's environment is independent domain, need to configure authentication port number as 389 when adding the LDAP server. Otherwise, if the domain contains child domains, such as ssl.sangfor.com, iam.sangfor.com for the root domain sangfor.com, the port number need to be configured to 3268, IP address need to configure to root domain IP.
- d) After configure the domain server, domain OU will automatically synchronize to IAM local database, and this action will be performed automatically for each 60 minutes. If the domain users or OU has been modified and the changes need to be applied to IAM immediately, click on the **"Sync with all LDAP servers"** as shown in the figure below :



- e) If AD domain is not enabled with **"LDAPS signing requirement service"**, **"LDAPS server certificate installation service"**, in IAM no need to configure **"enable encryption"**.

If needed:

**[Enable encryption]:** In September 2019, Microsoft announced in the security bulletin [ADV190023 | Microsoft Guidance for Enabling LDAP Channel Binding and LDAP Signing] that LDAP channel binding and LDAP signing will be enabled on the Active Directory server through the security update method (KB patch) in mid-January 2020. The security of Active Directory domain controllers can be significantly improved by configuring the server to reject Simple Authentication and Security Layer (SASL) LDAP binds that do not request signing (integrity verification) or to reject LDAP simple binds that are performed on a clear text (non-SSL/TLS-encrypted) connection. SASLs may include protocols such as the Negotiate, Kerberos, NTLM, and Digest protocols. To fulfill the requirement of security for Sangfor IAM, Sangfor



IAM supports for encryption docking.

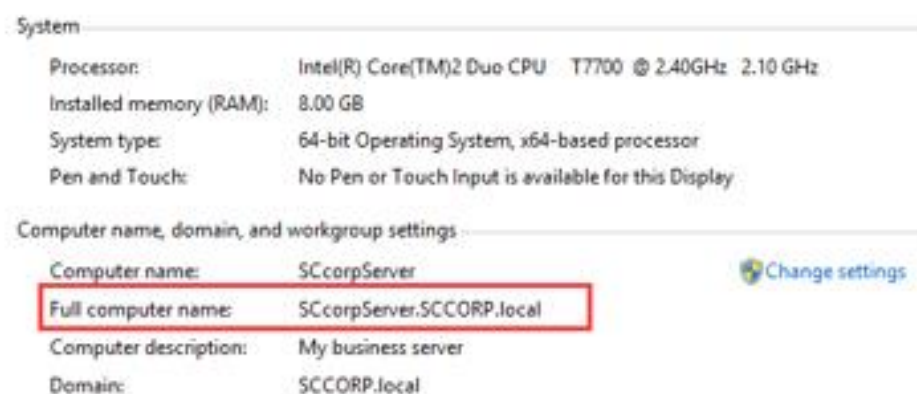
Official configuration by Microsoft:

<https://support.microsoft.com/en-us/help/935834/how-to-enable-ldap-signing-in-windows-server>

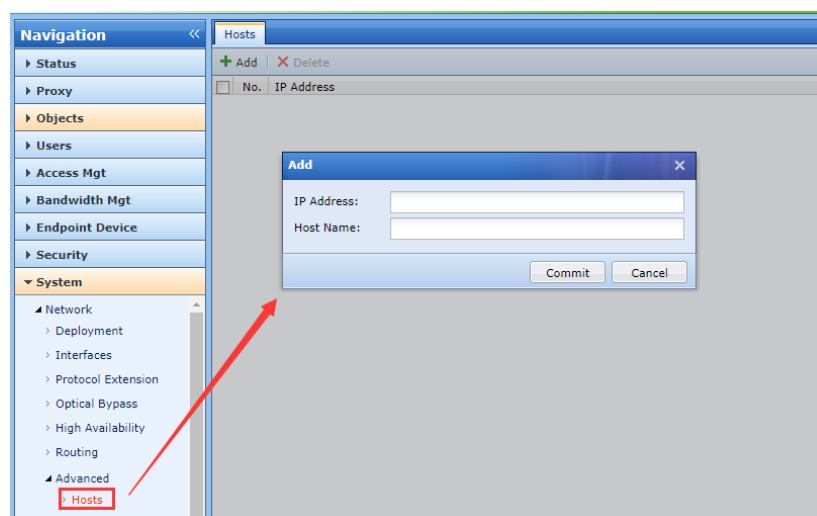
Encryption method: If the AD domain server is configured with [LDAPS signing requirement option], **it is recommended to choose TLS as the encryption method** (Microsoft supports SSL and TLS. After the AD domain enables the signature option, IAM can only connect to AD through encryption. **In particular, Windows 2000/2003/2008 do not support TLS encryption, only SSL encryption can be used**).

- When encryption docking is not enabled, the default port is 389.
- If encryption docking is enabled, when the encryption method is SSL, the authentication port is 636.
- If encryption docking is enabled, when the encryption method is TLS, the authentication port is 389.

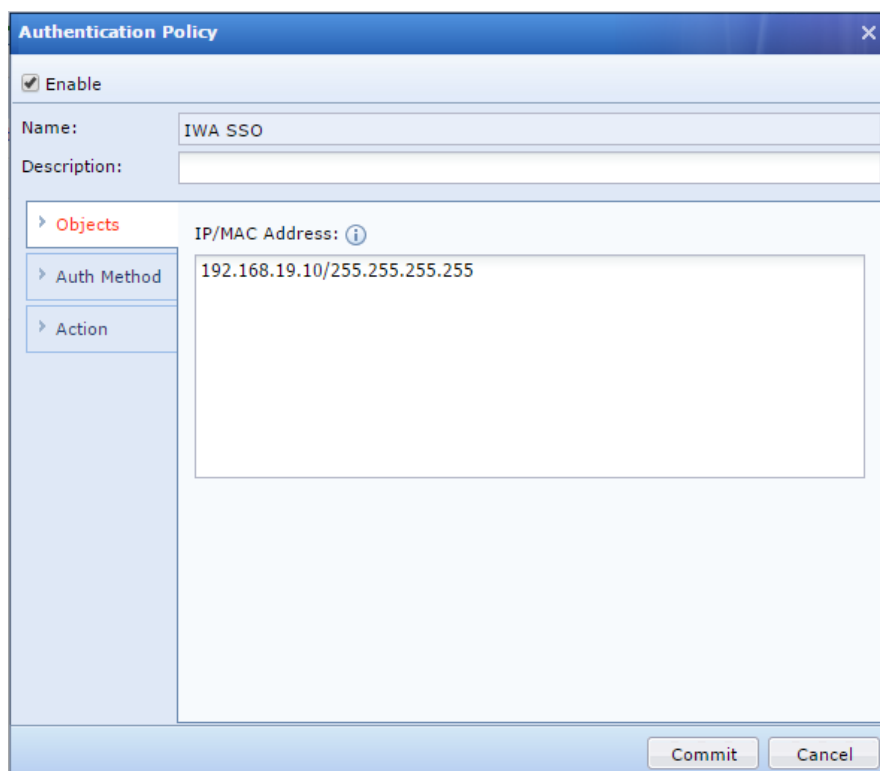
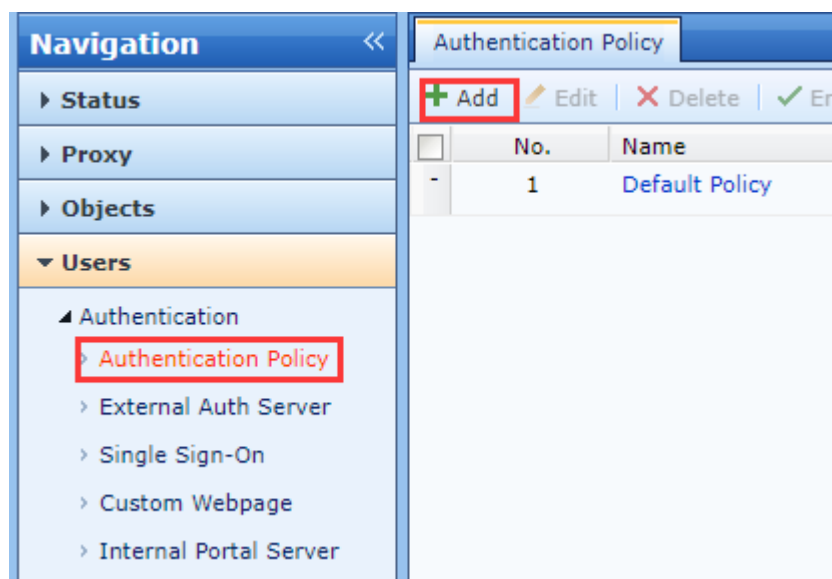
Verify certificate: If the AD domain server is configured with [LDAPS signing requirement option], you need to configure this item, fill in the domain name [AD domain server full computer name], and import the certificate.



Configure hosts: HOSTS resolves the domain name to the IP of the AD domain server.



2. Add a new authentication policy.



**Authentication Policy**

☒ Enable

Name: IWA SSO

Description:

Objects

**Auth Method**

Action

Auth Method:

- ☐ Open authentication
- ☐ Password based
- ☒ Single Sign-On(SSO)
- ☐ None (requests are rejected always)

SSO Enabled: ☒ AD server

[SSO Settings](#)

For User Fails SSO

- ☐ Open authentication
- ☒ Password based
  - Auth Server: 192.168.20.88
  - Captive Portal: [Preview](#)
  - Login Redirection: [Previously visited webpage](#)
- ☐ Go to [Predefined webpage](#)
- ☐ CAS server

Back Next

**Authentication Policy**

☒ Enable

Name: IWA SSO

Description:

Objects

Auth Method

**Action**

Add Non-Local/Domain Users To Group: [i](#)

/default/ [i](#)

☐ Add user account to local user database [i](#)

☐ Automatic binding

[Advanced](#)

Commit Cancel

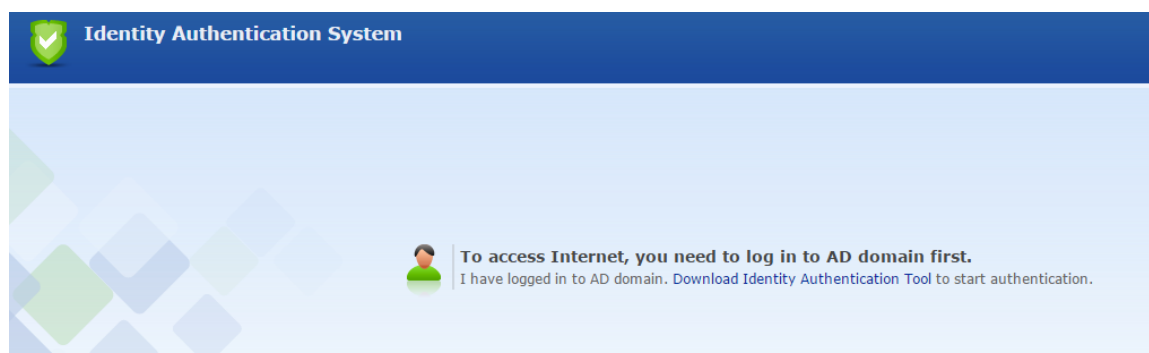
**[Note]**

① There are four handling methods for user who failed SSO authentication as shown in the “Auth Method” -> “For User Fails SSO” page; which are “Open authentication”, “Password based”, “Go to” and “CAS server”. These methods can be configured based on user requirement.

If admin allow internet access for SSO authentication failed users, select “Open authentication” to prevent re-authenticate again.

If requirement is to log activity for all authenticated users based on user name in domain, select “Password based” method to meet the requirement.

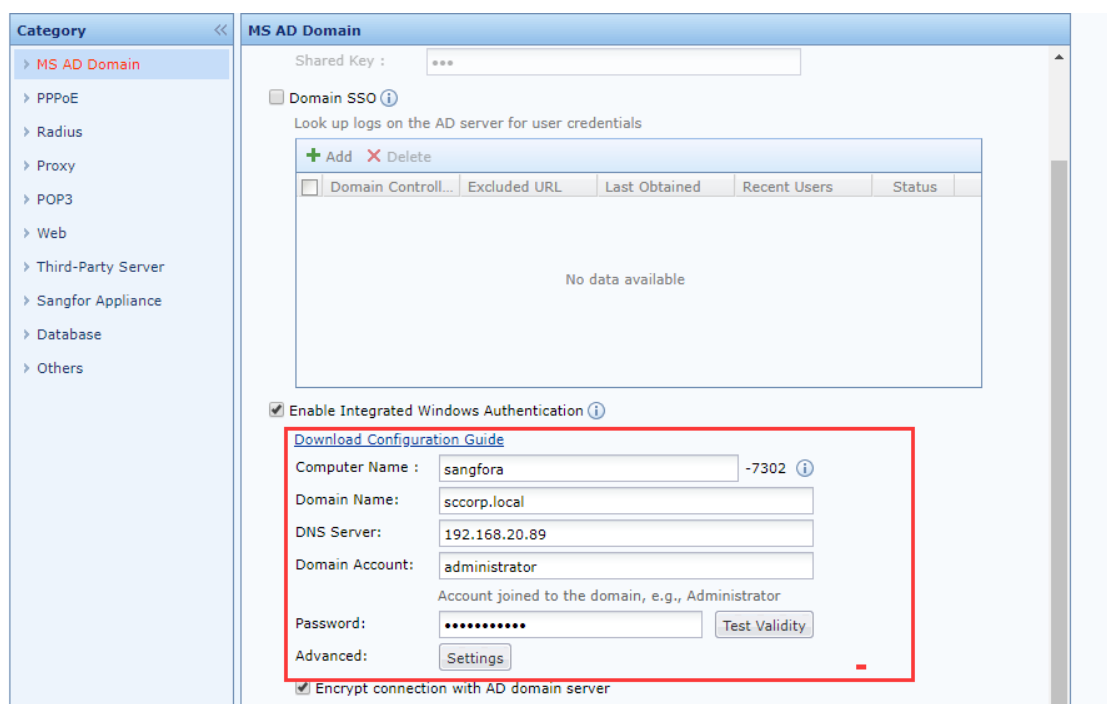
Other than that, if user requirements is to log internet activity, can select also option “Go to” and choose “predefined web page”. Domain users who failed in SSO authentication will be redirect to a custom web page as shown below to download Identity Authentication Tool and execute it for authentication purpose.



When the user has strict authentication requirements, that is, all Internet logs generated by the user must undergo CAS authentication, then select "CAS server". If single sign-on fails, CAS third-party authentication is used.

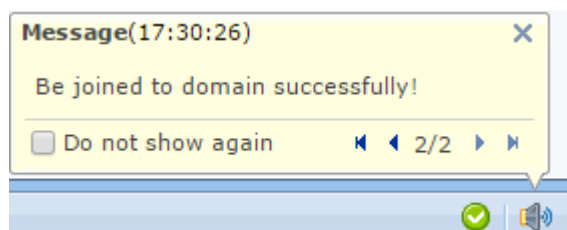
### 3. Configure IWA SSO option

The domain account used for IAM to join domain must have privilege to add workstation into domain such as administrator user account as shown below:



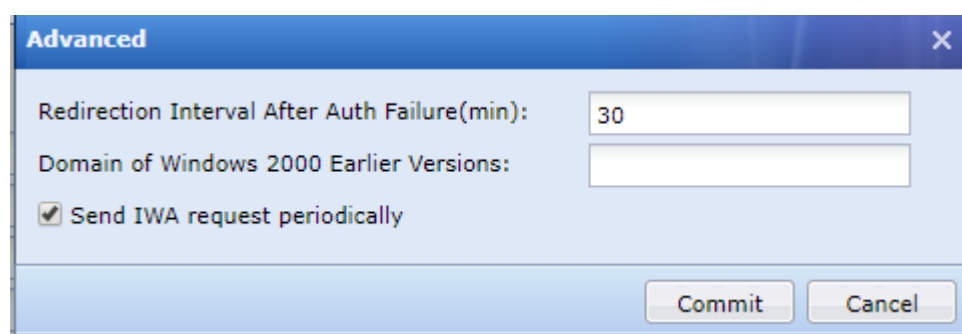
Note: When "Server Signing Requirement" is not enabled in the AD domain, it is not necessary to check "encrypt connection with AD domain server".

The message below is shown after click on Commit button and join domain successfully:



**[Note]**

- a) The domain account configure in IAM IWA SSO must have privilege to add workstation into domain, recommend to use administrator account, regular domain account can add workstation into domain but can add only 10 times. If cannot provide administrator account and regular domain user account fail to add, can create a new user account for testing.
- b) Then Advanced settings of IWA SSO configuration is shown below:



IWA SSO authentication require http redirection (this process is transparent to users), the figure above shows the redirection interval after auth failure (default is set to 30 min), if the SSO failure handling method is set to "Open authentication", recommend to change the value to 5min, otherwise, keep the default settings.

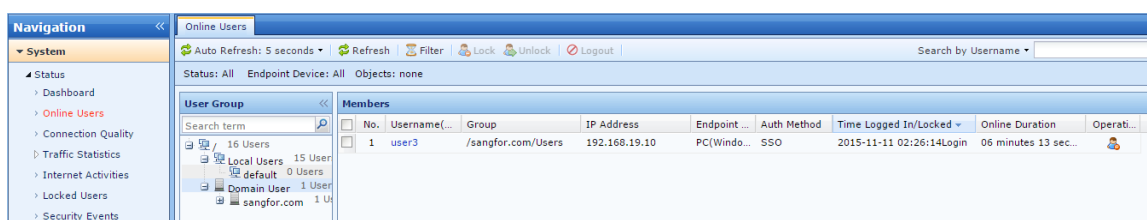
For domain Windows 2000 and before : windows 2003 until latest version, in order to compatible with domain in windows 2000, need to define the windows 2000 domain name during setup domain. If the domain name for Windows 2000 and Windows 2003 are different, need to add the domain name into the setting "Domain of Windows 2000 Earlier Versions" as shown in the figure above. If the Windows 2003 domain prefix is same with the domain name in Windows 2000, then no need to add into the configuration.

After the configuration is done, proceed to the next section for testing result.

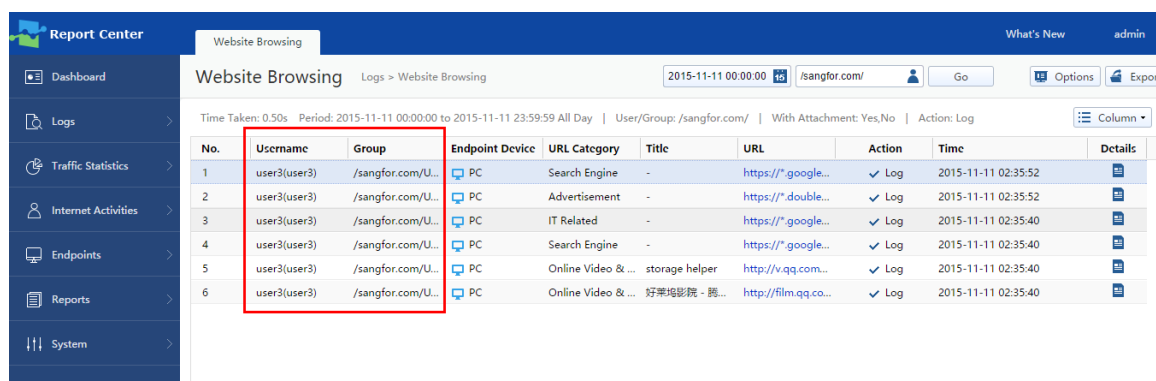
## Chapter 5 Testing Result

The result is shown as below:

1. When user login to domain with IWA SSO in IAM, browsing website will not require user to perform authentication again. The user details can be viewed in Online User list of IAM and it is shown as SSO in the figure below:

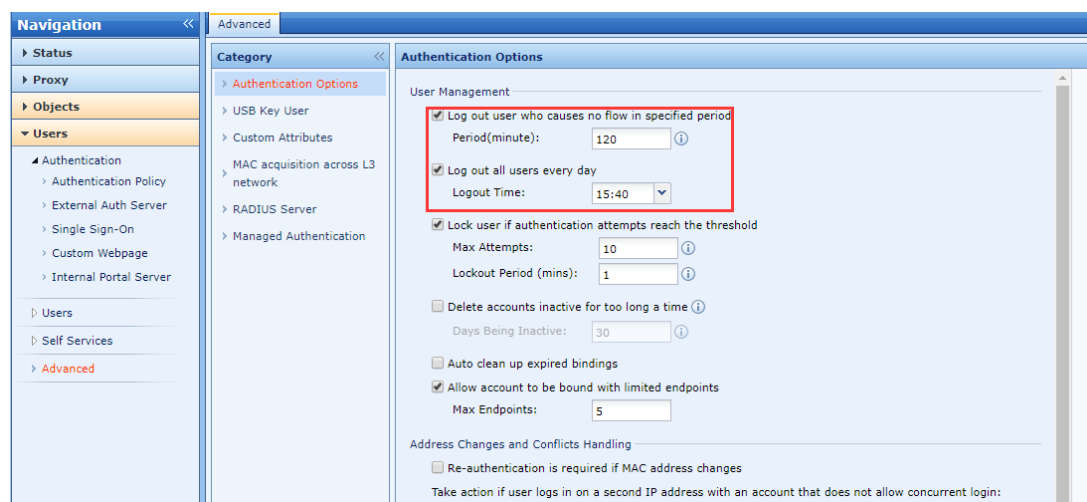


2. After PC online via SSO method, the logs in data center recorded user activities under their domain user name.

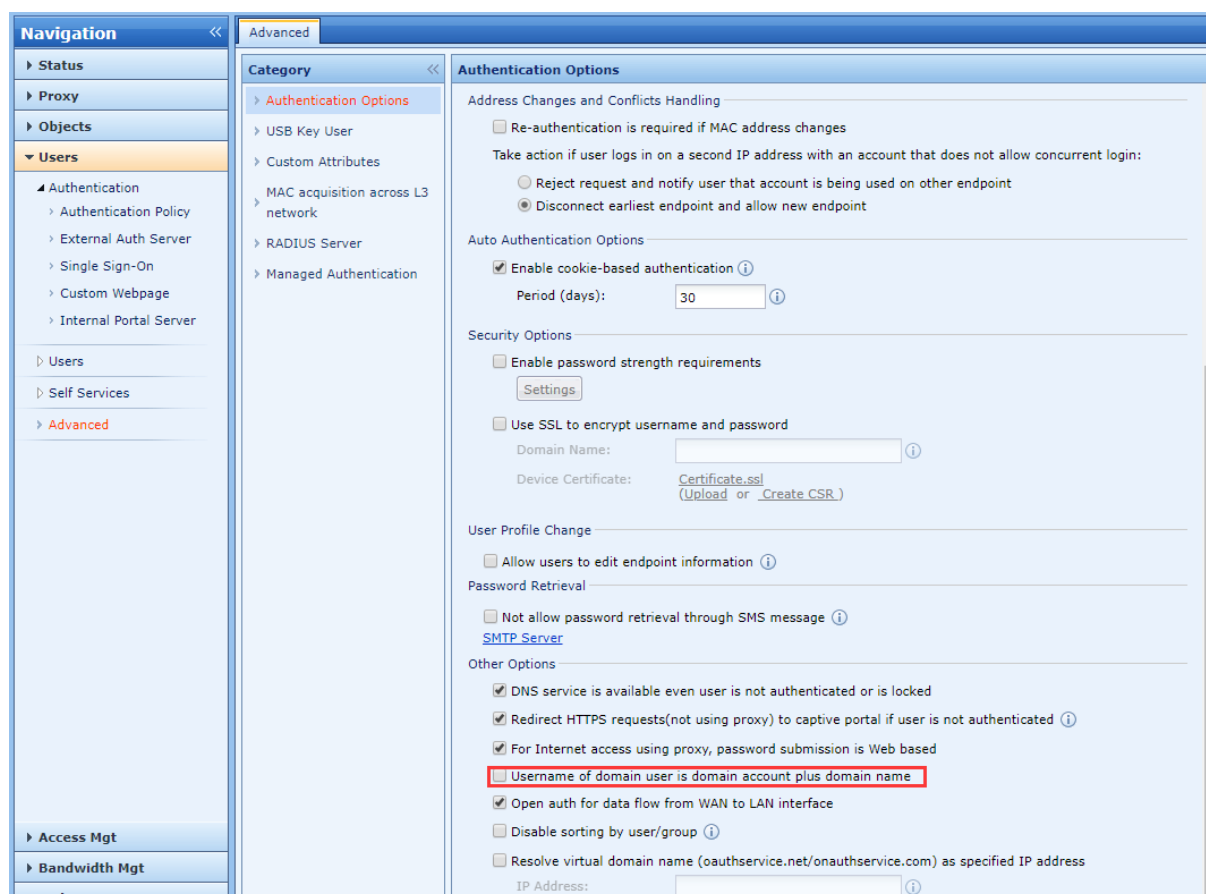


## Chapter 6 Precautions

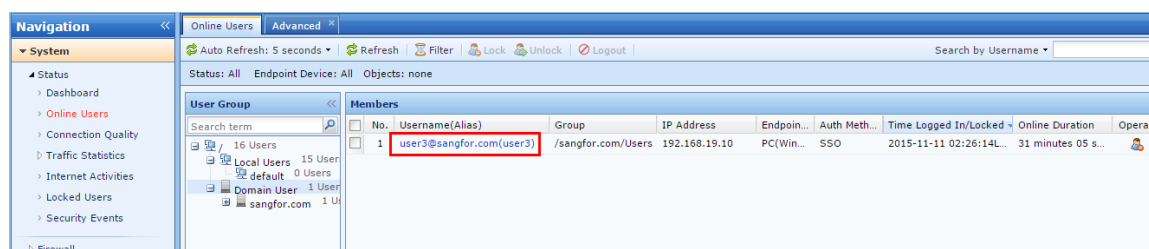
1. IWA SSO authentication not support online user logout in IAM when domain users logoff their PCs. However we can use the log out options under “Authentication Options” page to log out those users.



- If customer has multiple independent domains and all domains are sync with IAM, configure the option as shown in the figure below to identify users which has the same user name in different domains.



Enable the option and IAM will automatically add @domain name in online user list such support@sangfor.com as shown below:



- For SSO authentication, endpoint device must generate traffics and flowing through IAM , then only the user details (username, IP address) will be shown in online user list. IAM backend process will perform checking for each 10 minutes, if there is no traffics detected, the user will not been added into online user list.
- If AD server located at the WAN zone of IAM, and domain PC not able to logon to domain as usual, then the IP address of domain server need to be added into global excluded address in IAM due to PC traffics unable to pass through IAM before authentication.

5. In IWA authentication, after IAM joined domain, need to make sure domain PC able to telnet IAM PC name with port 80.
6. With the signature service enabled, IAM can only connect to the AD domain through encryption. In particular, Windows 2000/2003/2008 does not support TLS encryption, and only SSL encryption can be used. Windows Server 2008 R2 and above support both TLS and SSL encryption.

## Chapter 7 Appendix A: LDAPS Configuration Guide

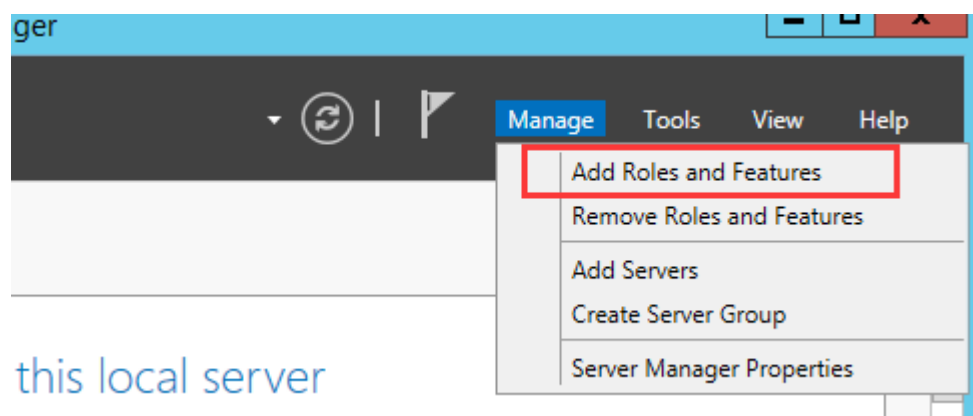
### 7.1 Background

In September 2019, Microsoft announced in the security bulletin [ADV190023 | Microsoft Guidance for Enabling LDAP Channel Binding and LDAP Signing] that LDAP channel binding and LDAP signing will be enabled on the Active Directory server through the security update method (KB patch) in mid-January 2020. The security of Active Directory domain controllers can be significantly improved by configuring the server to reject Simple Authentication and Security Layer (SASL) LDAP binds that do not request signing (integrity verification) or to reject LDAP simple binds that are performed on a clear text (non-SSL/TLS-encrypted) connection. SASLs may include protocols such as the Negotiate, Kerberos, NTLM, and Digest protocols.

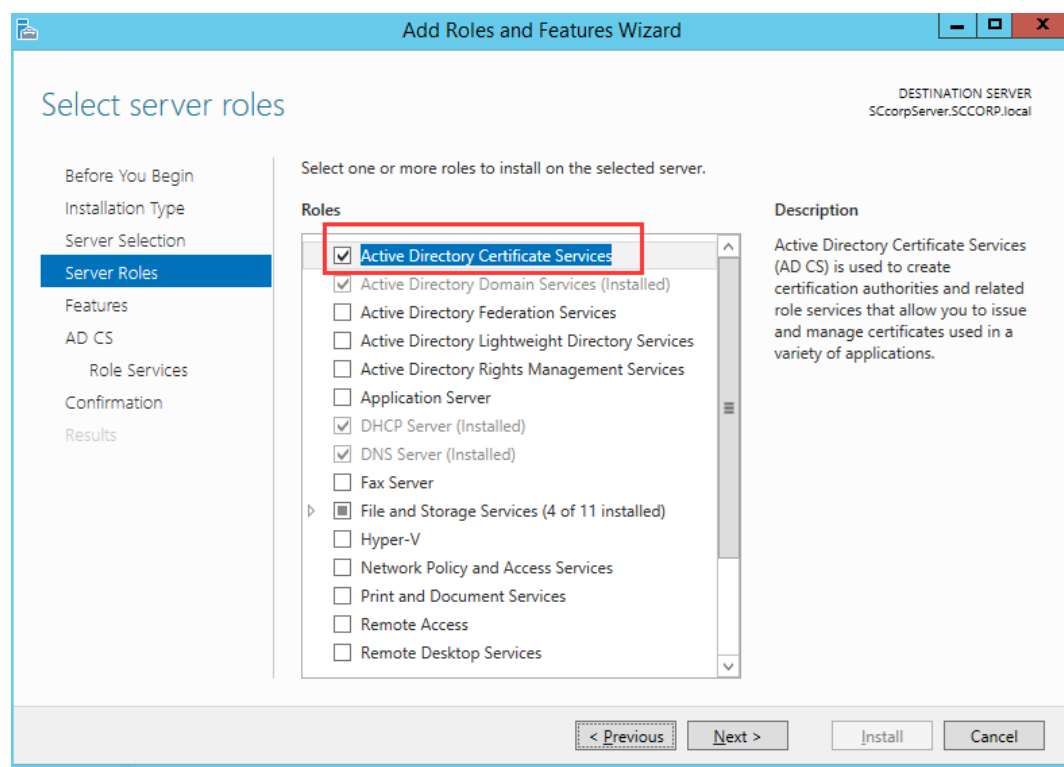
### 7.2 Configuration of Server Certificate Installation

After installing certificate service, the server root certificate can be exported for client certificate verification to enhance security. For how to install certificate service on the Active Directory server, refer to the following tutorial:

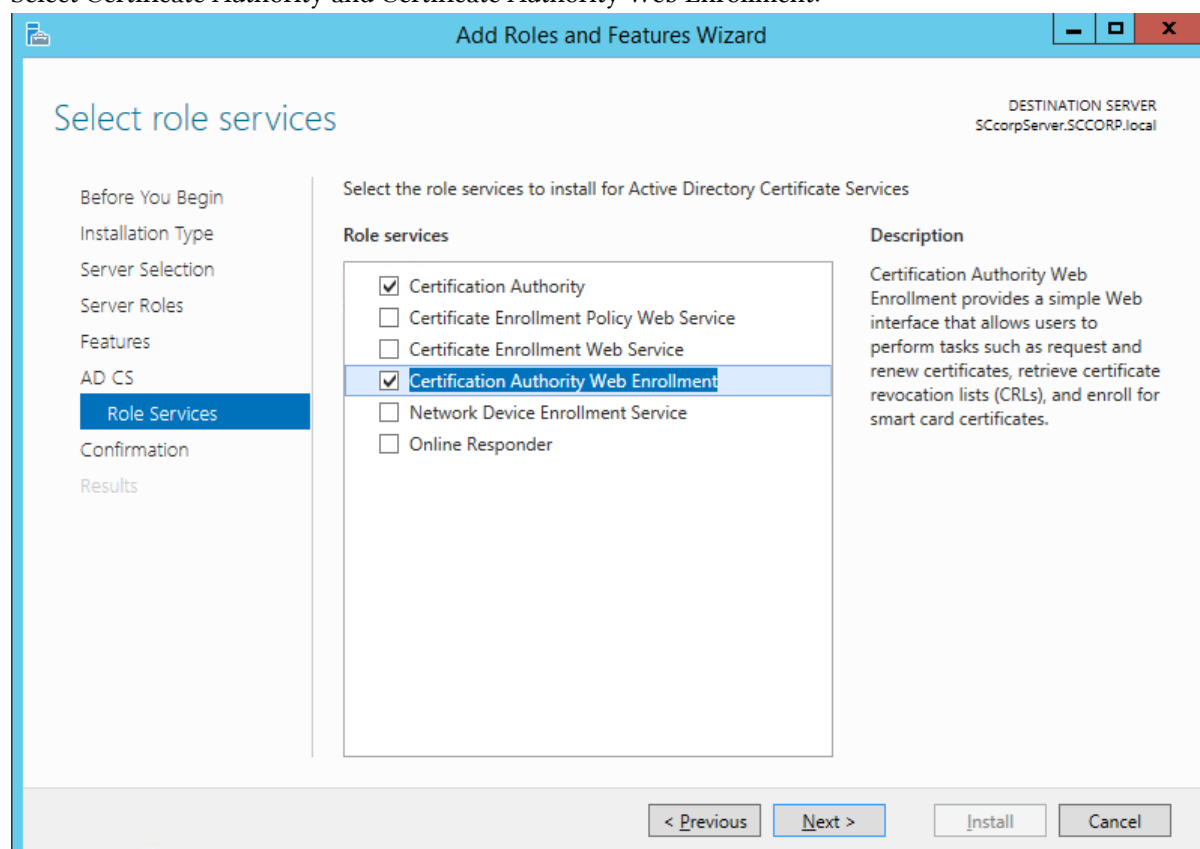
Open the Server Manager, right click add Roles and Features (using 2012 R2 to test), install Active Directory Certificate Services:



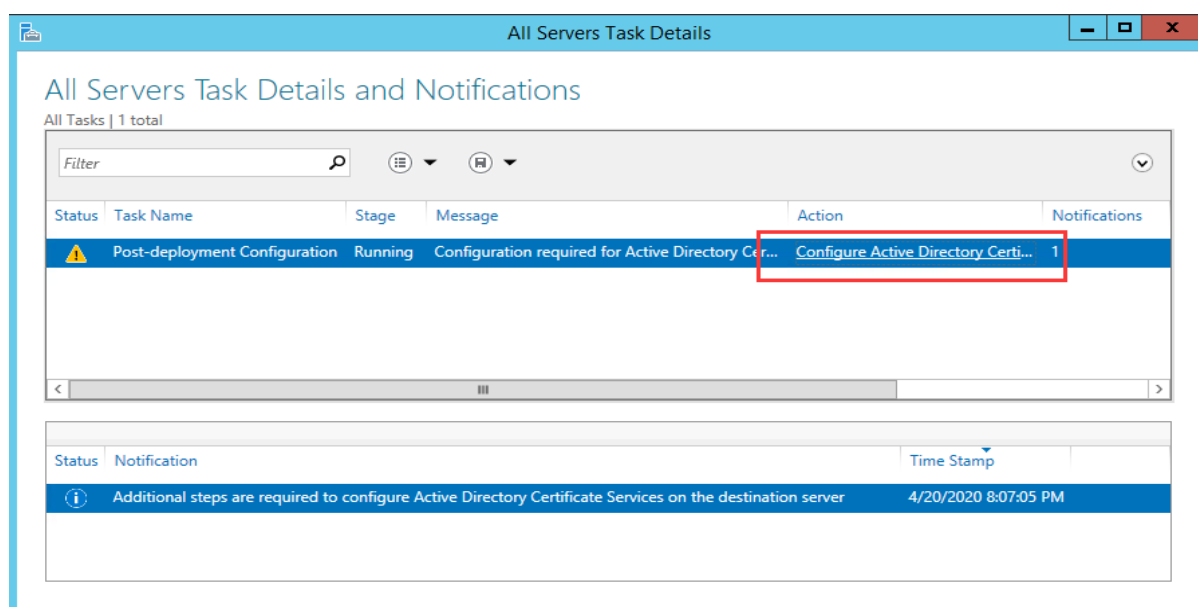
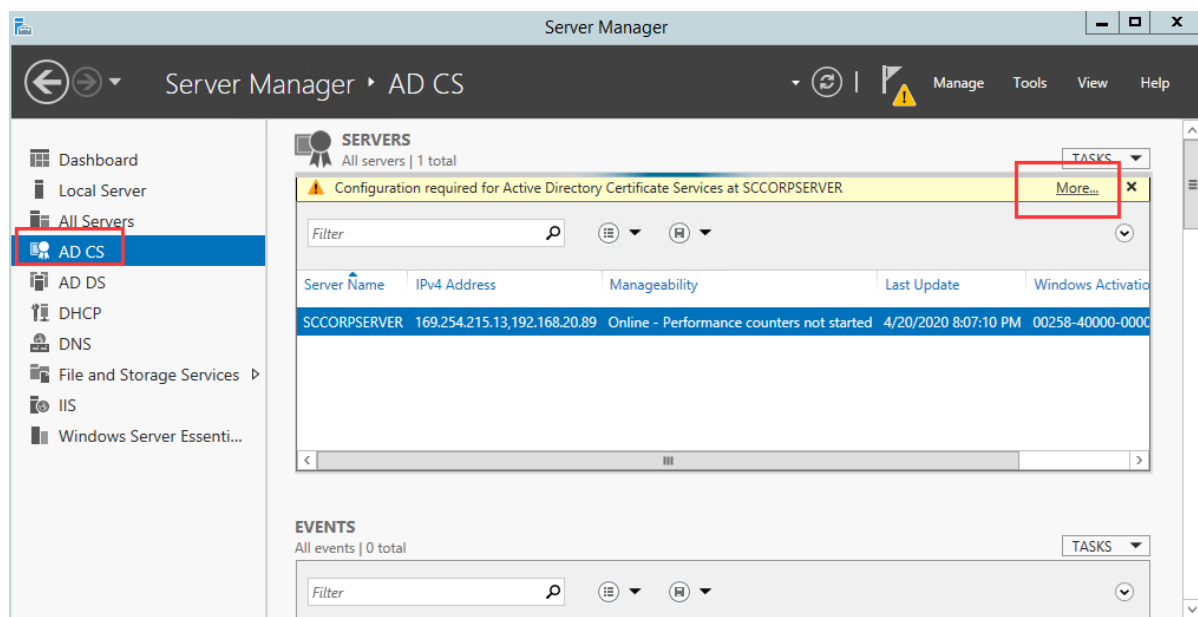




Select Certificate Authority and Certificate Authority Web Enrollment:



Go to AD CS, select more and click on Configure Active Directory Certification:



Select Enterprise CA:

The screenshot shows the 'AD CS Configuration' wizard at the 'Credentials' step. The left sidebar lists steps: Credentials (selected), Role Services, Setup Type, CA Type, Private Key, Cryptography, CA Name, Certificate Request, Certificate Database, Confirmation, Progress, and Results. The main area is titled 'Specify credentials to configure role services'. It lists two groups of role services: 'To install the following role services you must belong to the local Administrators group:' (Standalone certification authority, Certification Authority Web Enrollment, Online Responder) and 'To install the following role services you must belong to the Enterprise Admins group:' (Enterprise certification authority, Certificate Enrollment Policy Web Service, Certificate Enrollment Web Service, Network Device Enrollment Service). A 'Credentials' field contains 'SCCORP\administrator' with a 'Change...' button. The bottom navigation bar includes '< Previous', 'Next >', 'Configure', and 'Cancel'.

AD CS Configuration

DESTINATION SERVER  
SCcorpServer.SCCORP.local

### Credentials

Specify credentials to configure role services

To install the following role services you must belong to the local Administrators group:

- Standalone certification authority
- Certification Authority Web Enrollment
- Online Responder

To install the following role services you must belong to the Enterprise Admins group:

- Enterprise certification authority
- Certificate Enrollment Policy Web Service
- Certificate Enrollment Web Service
- Network Device Enrollment Service

Credentials:

[More about AD CS Server Roles](#)

< Previous   Next >   Configure   Cancel

The screenshot shows the 'AD CS Configuration' wizard at the 'Role Services' step. The left sidebar lists steps: Credentials, Role Services (selected), Setup Type, CA Type, Private Key, Cryptography, CA Name, Certificate Request, Certificate Database, Confirmation, Progress, and Results. The main area is titled 'Select Role Services to configure'. It lists several services with checkboxes: Certification Authority (checked), Certification Authority Web Enrollment (checked), Online Responder (unchecked), Network Device Enrollment Service (unchecked), Certificate Enrollment Web Service (unchecked), and Certificate Enrollment Policy Web Service (unchecked). The bottom navigation bar includes '< Previous', 'Next >', 'Configure', and 'Cancel'.

AD CS Configuration

DESTINATION SERVER  
SCcorpServer.SCCORP.local

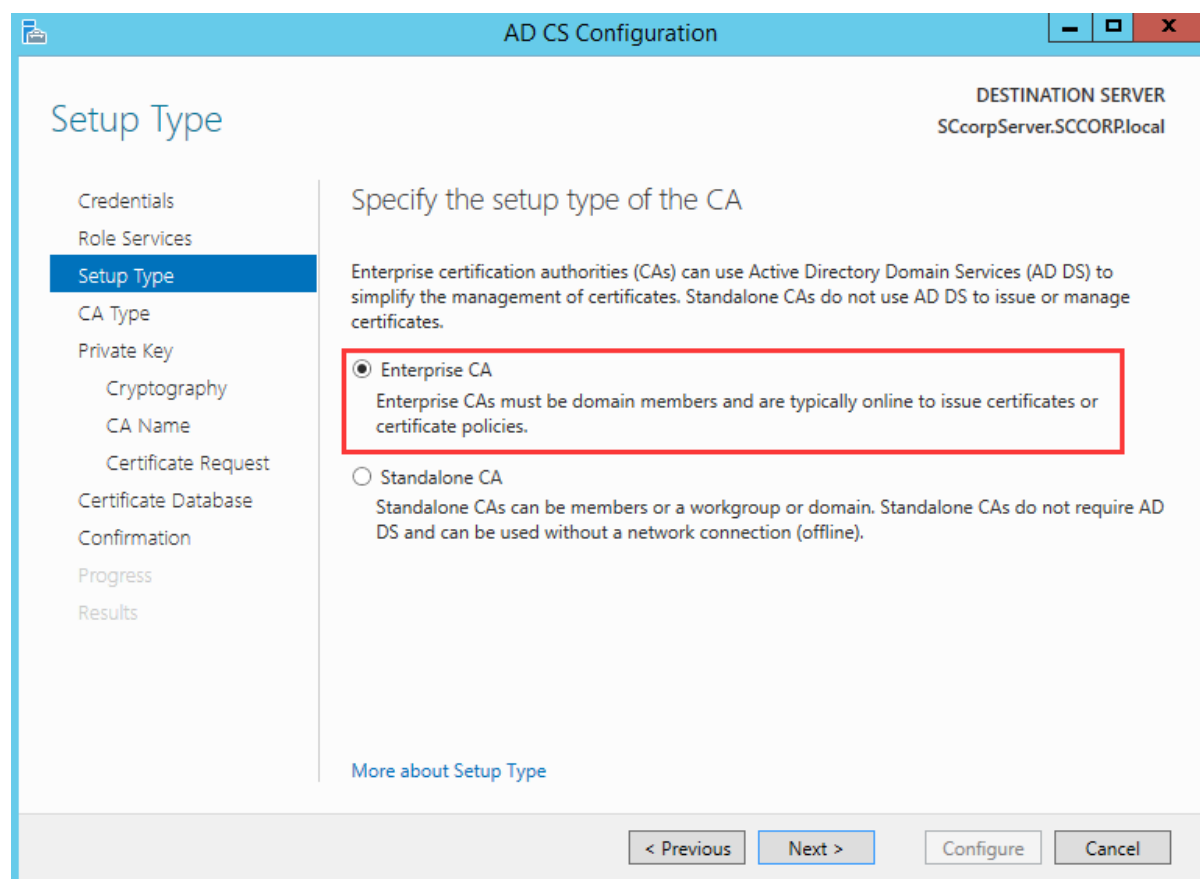
### Role Services

Select Role Services to configure

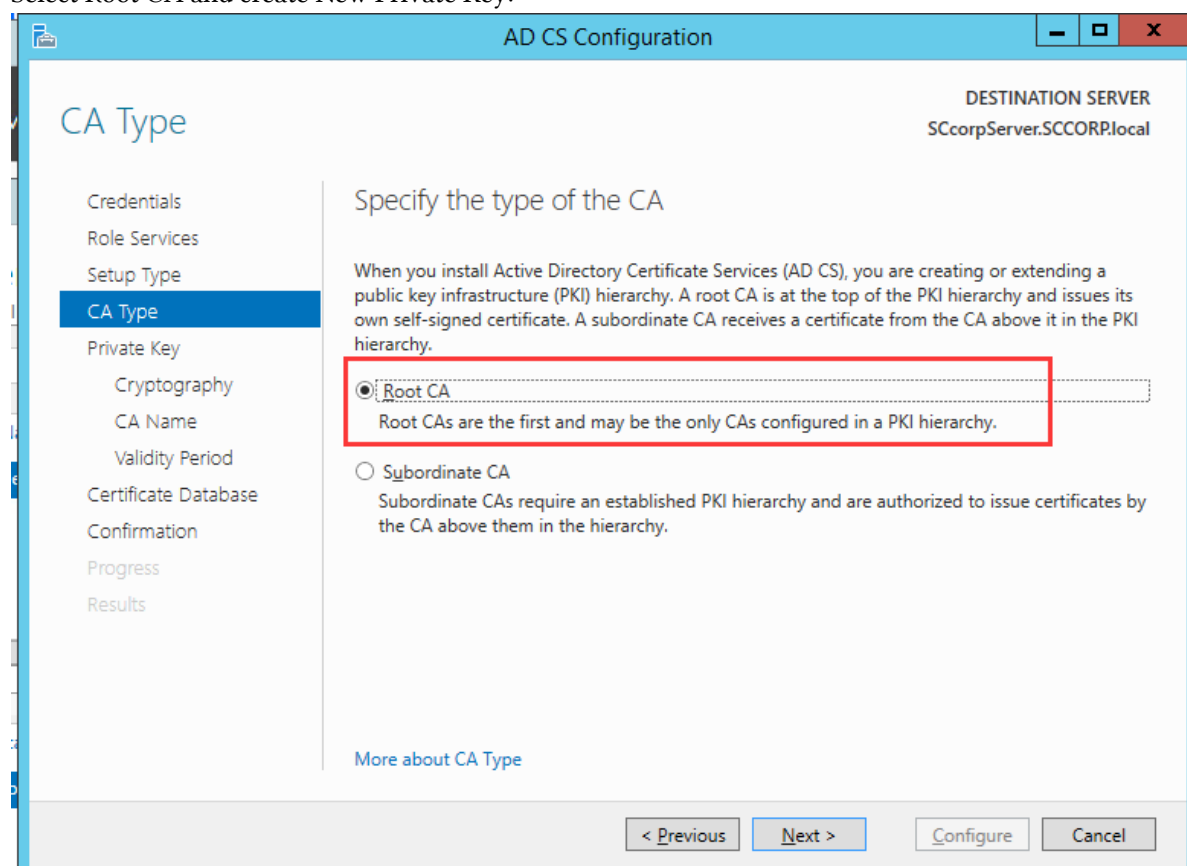
- ☒ Certification Authority
- ☒ Certification Authority Web Enrollment
- ☐ Online Responder
- ☐ Network Device Enrollment Service
- ☐ Certificate Enrollment Web Service
- ☐ Certificate Enrollment Policy Web Service

[More about AD CS Server Roles](#)

< Previous   Next >   Configure   Cancel



Select Root CA and create New Private Key:



The screenshot shows the 'Private Key' step of the AD CS Configuration wizard. The left sidebar contains a list of steps: Credentials, Role Services, Setup Type, CA Type, Private Key (highlighted), Cryptography, CA Name, Validity Period, Certificate Database, Confirmation, Progress, and Results. The main area is titled 'Specify the type of the private key'. It includes a sub-header 'To generate and issue certificates to clients, a certification authority (CA) must have a private key.' and three radio button options: 'Create a new private key' (selected), 'Use existing private key', and 'Select a certificate and use its associated private key'. Below these options are detailed instructions for each. At the bottom, there are buttons for '< Previous', 'Next >', 'Configure', and 'Cancel'. The top right corner shows the 'DESTINATION SERVER' as 'SCcorpServer.SCCORP.local'.

AD CS Configuration

DESTINATION SERVER  
SCcorpServer.SCCORP.local

### Private Key

Credentials  
Role Services  
Setup Type  
CA Type  
**Private Key**  
Cryptography  
CA Name  
Validity Period  
Certificate Database  
Confirmation  
Progress  
Results

#### Specify the type of the private key

To generate and issue certificates to clients, a certification authority (CA) must have a private key.

- ☒ **Create a new private key**  
Use this option if you do not have a private key or want to create a new private key.
- ☐ **Use existing private key**  
Use this option to ensure continuity with previously issued certificates when reinstalling a CA.
  - ☐ **Select a certificate and use its associated private key**  
Select this option if you have an existing certificate on this computer or if you want to import a certificate and use its associated private key.
  - ☐ **Select an existing private key on this computer**  
Select this option if you have retained private keys from a previous installation or want to use a private key from an alternate source.

[More about Private Key](#)

< Previous   Next >   Configure   Cancel

Set the validity period:

The screenshot shows the 'Validity Period' step of the AD CS Configuration wizard. The left sidebar contains a list of steps: Credentials, Role Services, Setup Type, CA Type, Private Key, Cryptography, CA Name, Validity Period (highlighted), Certificate Database, Confirmation, Progress, and Results. The main area is titled 'Specify the validity period'. It includes a sub-header 'Select the validity period for the certificate generated for this certification authority (CA):' and a text input field with '100' and a dropdown menu set to 'Years'. Below this, it shows the 'CA expiration Date: 4/20/2120 8:15:00 PM'. A note states: 'The validity period configured for this CA certificate should exceed the validity period for the certificates it will issue.' At the bottom, there are buttons for '< Previous', 'Next >', 'Configure', and 'Cancel'. The top right corner shows the 'DESTINATION SERVER' as 'SCcorpServer.SCCORP.local'.

AD CS Configuration

DESTINATION SERVER  
SCcorpServer.SCCORP.local

### Validity Period

Credentials  
Role Services  
Setup Type  
CA Type  
Private Key  
Cryptography  
CA Name  
**Validity Period**  
Certificate Database  
Confirmation  
Progress  
Results

#### Specify the validity period

Select the validity period for the certificate generated for this certification authority (CA):

100   Years

CA expiration Date: 4/20/2120 8:15:00 PM

The validity period configured for this CA certificate should exceed the validity period for the certificates it will issue.

[More about Validity Period](#)

< Previous   Next >   Configure   Cancel

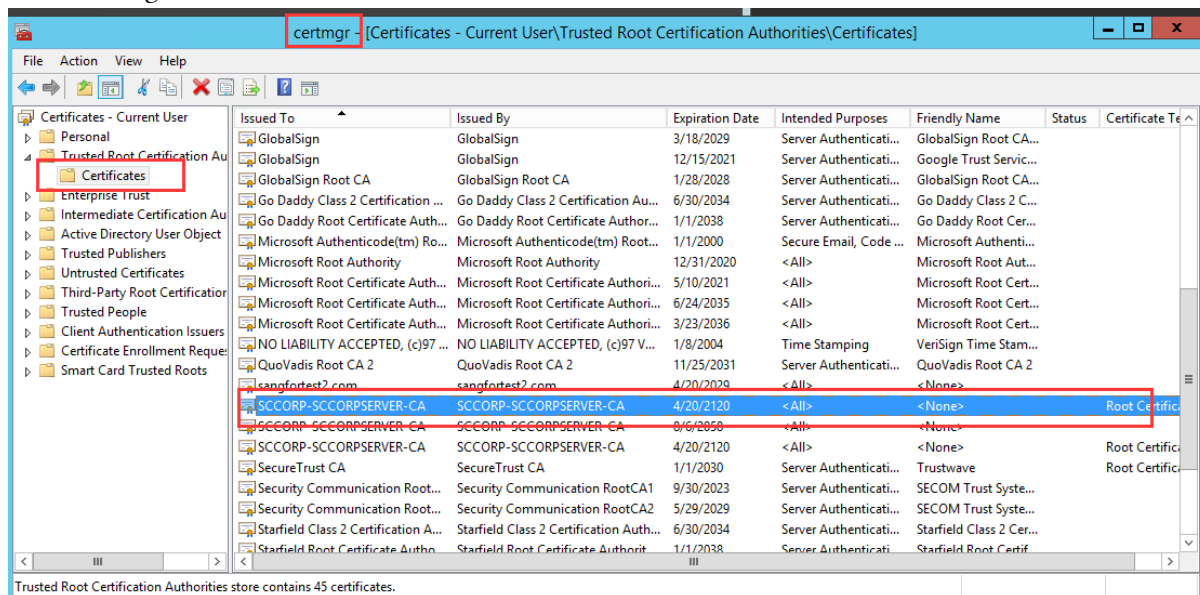
Specify the database location:

The screenshot shows the 'AD CS Configuration' window with the 'CA Database' step selected in the left-hand navigation pane. The main area is titled 'Specify the database locations'. It contains two text input fields: 'Certificate database location:' and 'Certificate database log location:', both of which have the value 'C:\Windows\system32\CertLog' entered. At the top right, it says 'DESTINATION SERVER SCcorpServer.SCCORP.local'. At the bottom, there are buttons for '< Previous', 'Next >', 'Configure', and 'Cancel'. A link 'More about CA Database' is also present.

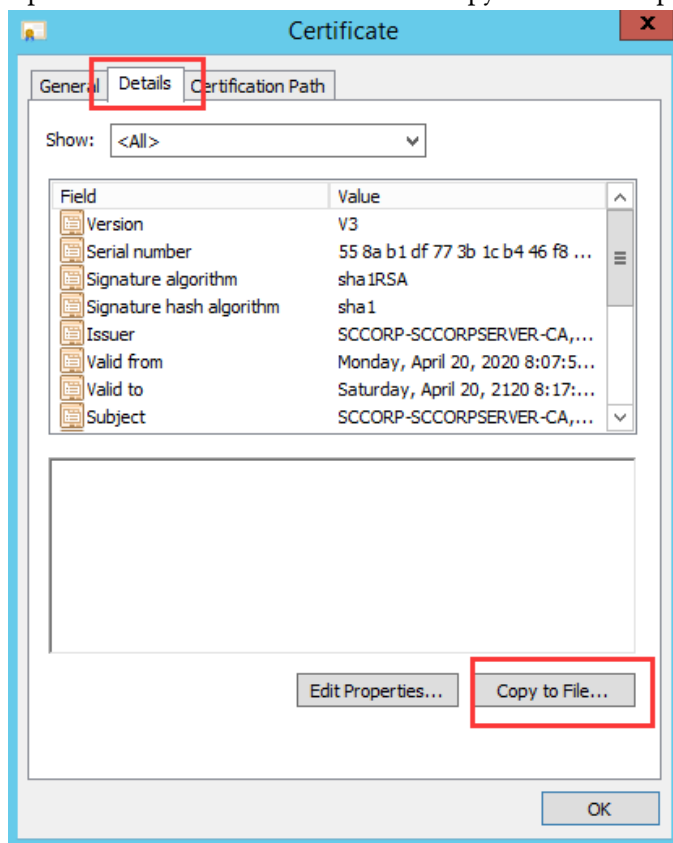
Installation complete:

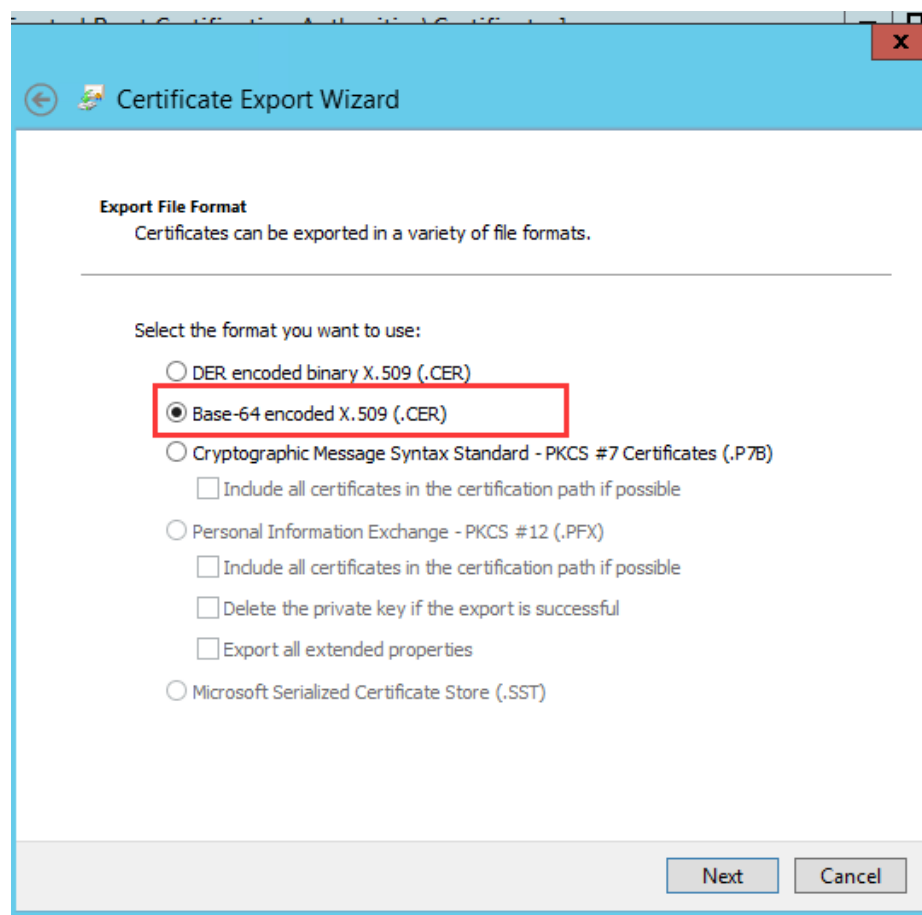
The screenshot shows the 'AD CS Configuration' window with the 'Results' step selected in the left-hand navigation pane. The main area is titled 'Results' and displays a summary of the configuration. It states 'The following roles, role services, or features were configured:' followed by a section titled 'Active Directory Certificate Services'. Under this section, two items are listed: 'Certification Authority' and 'Certification Authority Web Enrollment'. Both items have a green checkmark icon and the text 'Configuration succeeded'. Below each item is a link to 'More about' its configuration. At the bottom, there are buttons for '< Previous', 'Next >', 'Close', and 'Cancel'. The 'DESTINATION SERVER SCcorpServer.SCCORP.local' is also displayed at the top right.

Go to certmgr.msc:



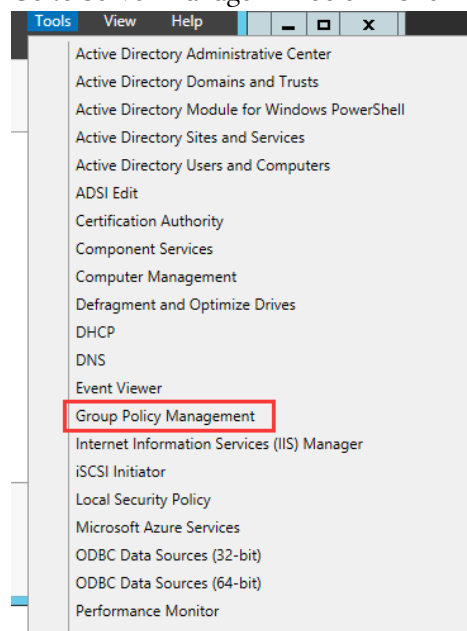
Open the cert and click on Details -> Copy to File and export as Base-64 with .cer format:





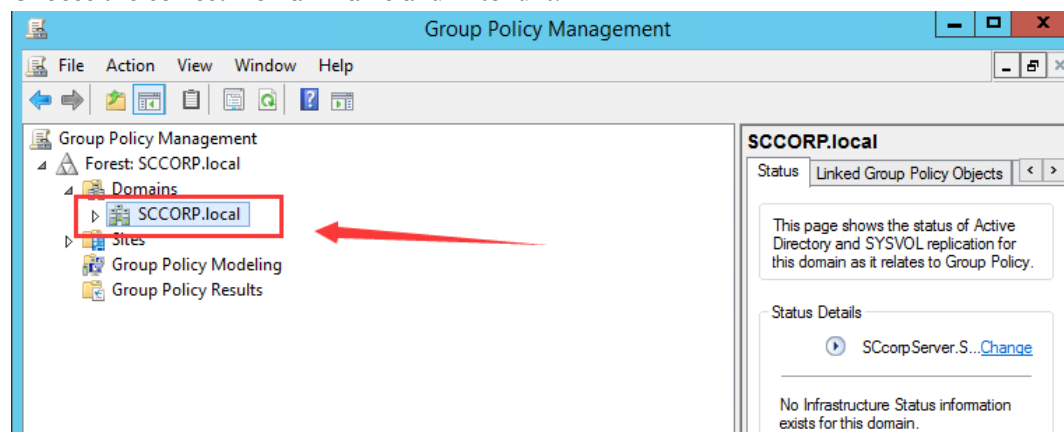
## 7.3 Configuration of LDAPS Server Signing

Go to Server Manager -> Tools -> Click Group Policy Management:

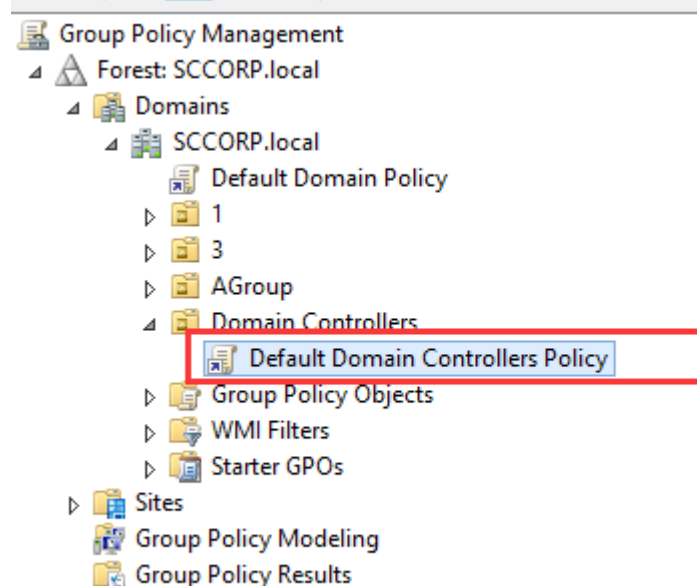




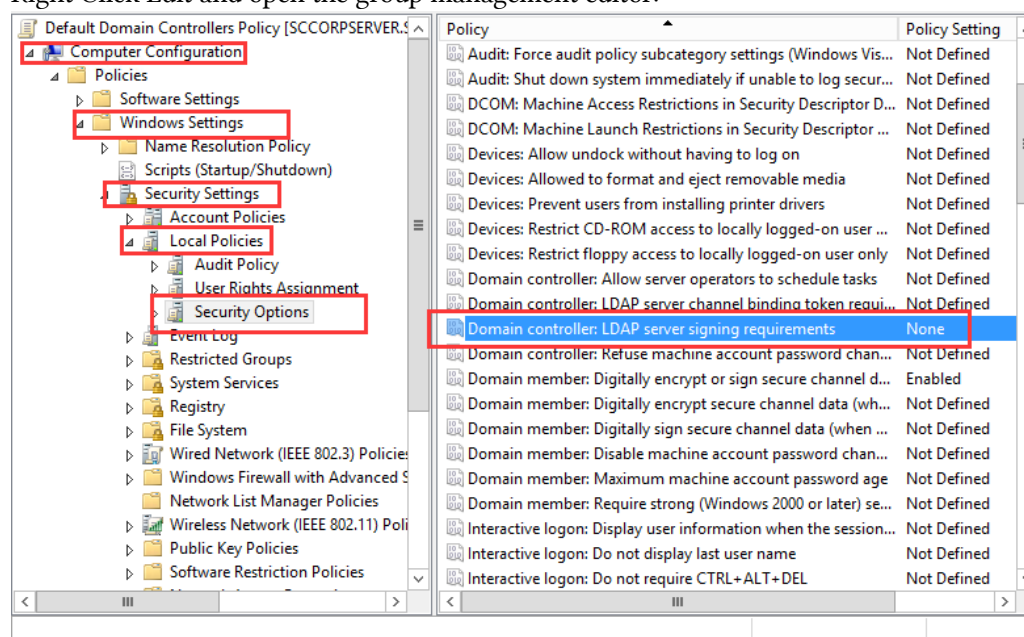
Choose the correct Domain name and Extend it.



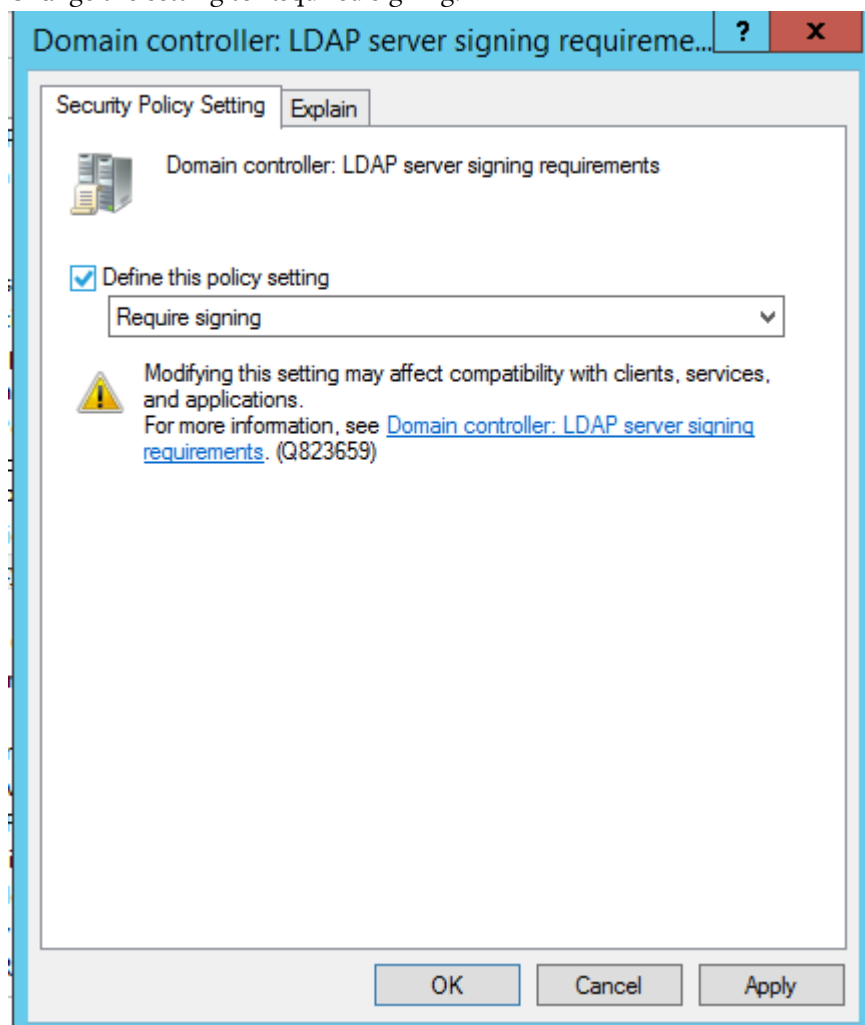
Choose the domain controller -> Select Default Domain controller Policy:




Right Click Edit and open the group management editor:



Change the setting to Required signing.



After configured, CMD run the gpupdate /force to push the group policy.

 Command Prompt

```
C:\Users\Administrator>
C:\Users\Administrator>gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.

C:\Users\Administrator>
```

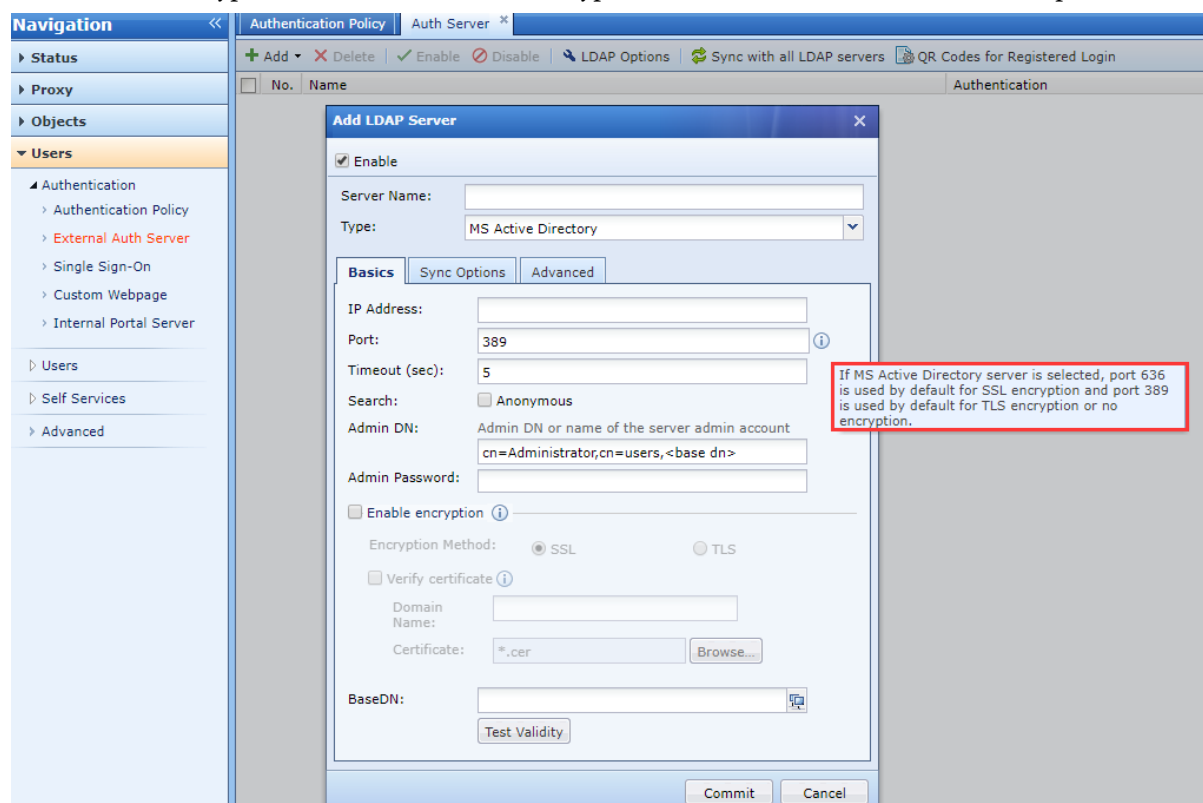
## 7.4 AD Configuration on IAM

The above are the configuration tutorial on the AD domain. This section describes the configuration of the AD domain server on IAM:

## 7.4.1 Authentication Port Description

As shown in the figure, the LDAP server is configured at the external authentication server to connect with the Microsoft AD domain:

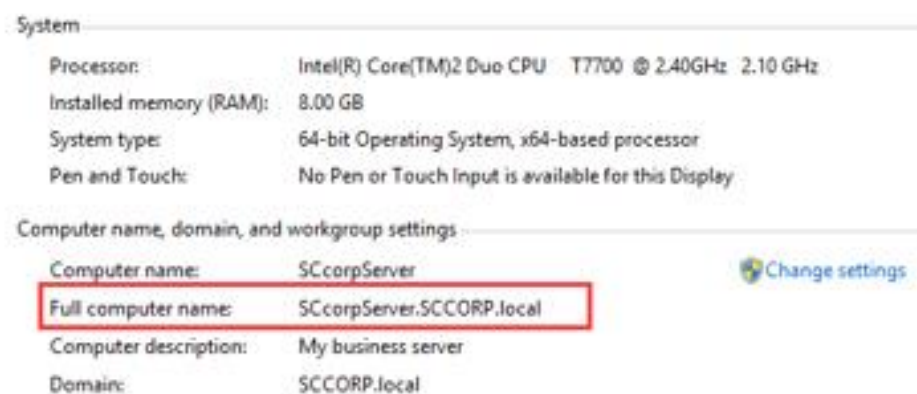
- When encryption is not enabled, the default port is 389.
- If encryption is enabled, when the encryption method is SSL, the authentication port is 636.
- If encrypted is enabled, when the encryption method is TLS, the authentication port is 389.



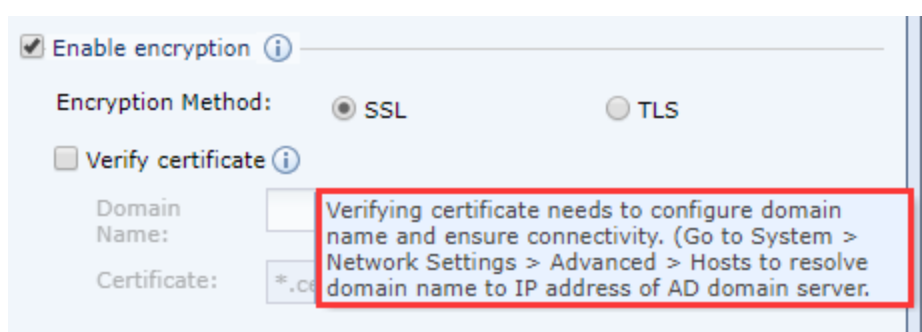
## 7.4.2 Enable Encryption

As shown in the figures below:

- The LDAP server can be configured not to enable encryption. In this scenario, the LDAP server signing requirement is not enabled on the Microsoft AD domain.
- If the AD domain has been configured to enable LDAP server signing requirement, then encryption must be turned on here. The encryption method can be selected by yourself, and the authentication port can be modified according to the selected encryption method as described above.
- The verify certificate function can be turned off, and it will not affect the connection with the AD domain with server signing requirement enabled.
- If the verify certificate function is enabled, you need to configure the domain name and import the certificate file:
  - The configuration of the domain name needs to be configured as the full computer name of the AD domain server: as shown below, you can log in to the AD domain server to obtain this field, as shown in the following figure:



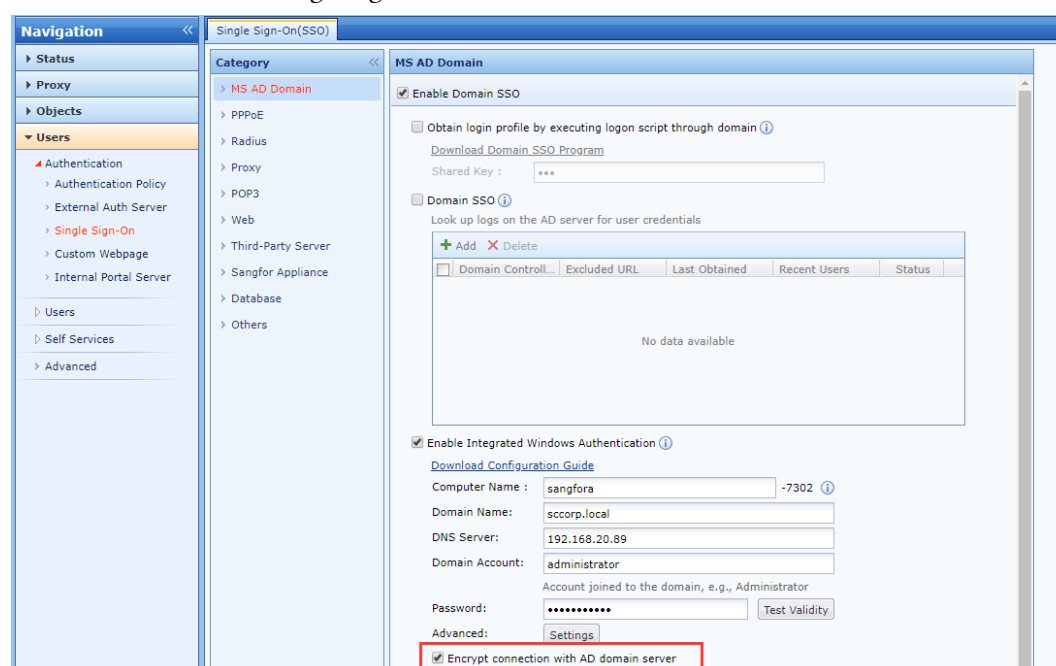
- After the domain name is configured, you need to add the host rule to resolve the filled domain name to the IP address of the AD domain server:



- Import the certificate. The certificate needs to be a Base64 encoded .cer format certificate exported from the root certificate file on the AD domain server. This is described in the [Configuration of Server Certification Installation] section and will not be repeated here.

## 7.5 IWA SSO Configuration

The IWA single sign-on function will be affected by the **server signing requirement** enabled in the AD domain. If the server signing requirement is enabled on the AD domain, you need to enable the encrypt connection at the IWA single sign-on location:





Copyright © SANGFOR Technologies Inc. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of SANGFOR Technologies Inc.

SANGFOR is the trademark of SANGFOR Technologies Inc. All other trademarks and trade names mentioned in this document are the property of their respective holders. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

The information in this document is subject to change without notice.

To obtain the latest version, contact the international service center of SANGFOR Technologies Inc