



SANGFOR

IAM

Panduan Konfigurasi IWA SSO

Versi 12.0.42

Catatan Perubahan

Tanggal	Deskripsi Perubahan
April 27, 2020	Rilis Dokumen Versi 12.0.42.

Daftar Isi

Bab 1 Latar Belakang Masalah	1
Bab 2 Solusi	1
2.1 IWA SSO Autentikasi	1
Bab 3 Lingkungan Pengujian	1
3.1 Topologi	1
Bab 4 Konfigurasi	2
Bab 5 Hasil Pengujian	11
Bab 6 Tindakan Pencegahan	11
Bab 7 Lampiran A: Panduan Konfigurasi LDAPS	13
7.1 Latar Belakang	13
7.2 Konfigurasi dari Instalasi Sertifikat Server	13
7.3 Konfigurasi dari LDAP Server Signing	21
7.4 Konfigurasi AD di IAM	23
7.4.1 Deskripsi Autentikasi Port	24
7.4.2 Enable Encryption	24
7.5 Konfigurasi IWA SSO	25

Bab 1 Latar Belakang Masalah

Lingkungan pelanggan memiliki AD domain untuk mengelola pengguna internal dan IT manajer ingin menerapkan Sangfor IAM di jaringan mereka untuk tujuan autentikasi pengguna. Manajer ingin sinkronisasi IAM dengan AD controller (Domain SSO) yang prosesnya transparan untuk pengguna internal sehingga pengguna tidak perlu memasukkan kembali log in detail lagi untuk autentikasi IAM. Berikut ini adalah beberapa rincian kebutuhan pelanggan:

1. Manajer berharap untuk melihat pengguna online dengan nama pengguna mereka di AD controller, kemudian mengaudit semua perilaku jaringan sesuai dengan nama pengguna.
2. Manajer tidak ingin mengubah domain GPO mereka dan oleh karena itu tidak mengizinkan domain SSO script mode (script mode diperlukan untuk menambahkan logon.exe dan logoff.exe ke domain) yang tidak sesuai dengan kebijakan keamanan perusahaan mereka.

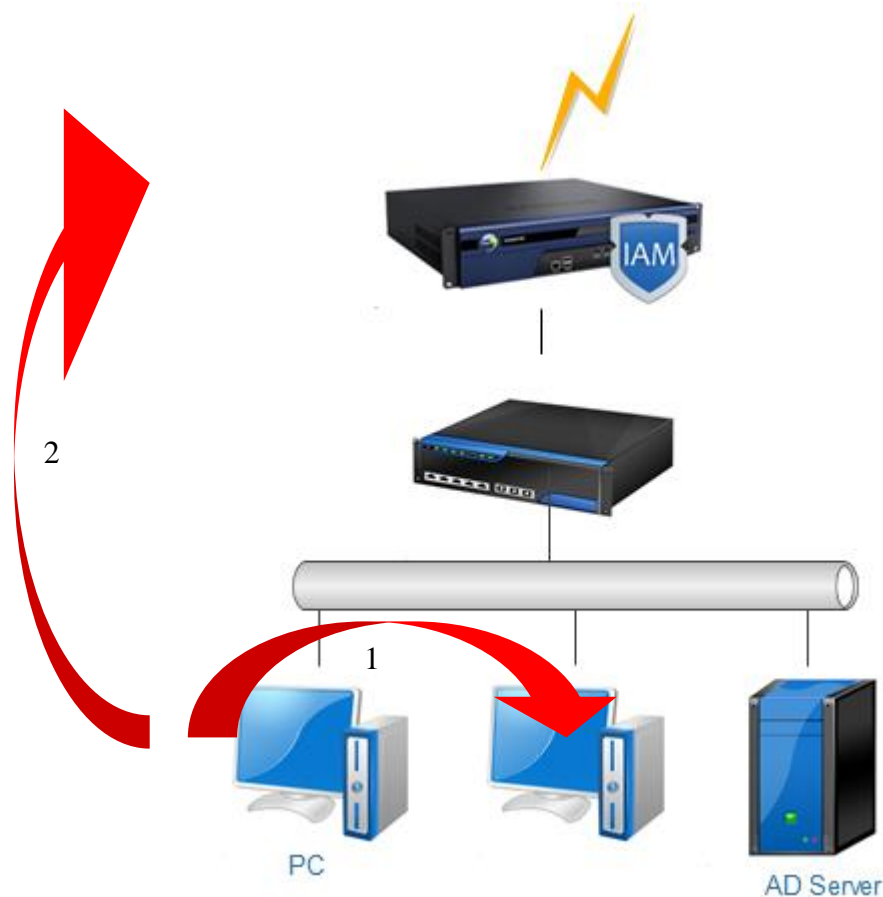
Bab 2 Solusi

2.1 IWA SSO Autentikasi

Dalam metode ini, Sangfor IAM akan bergabung ke dalam pelanggan windows domain dan bertindak sebagai resource di domain. Ketika domain PC log on ke domain dan menelusuri website, permintaan akan dihentikan oleh IAM dan dialihkan ke resource halaman IAM. Tindakan ini akan memicu kerberos autentikasi dan IAM akan memperoleh tiket kirim oleh domain PC kemudian mendapatkan rincian untuk IWA SSO autentikasi . Namun proses ini transparan untuk pengguna.

Bab 3 Lingkungan Pengujian

3.1 Topologi



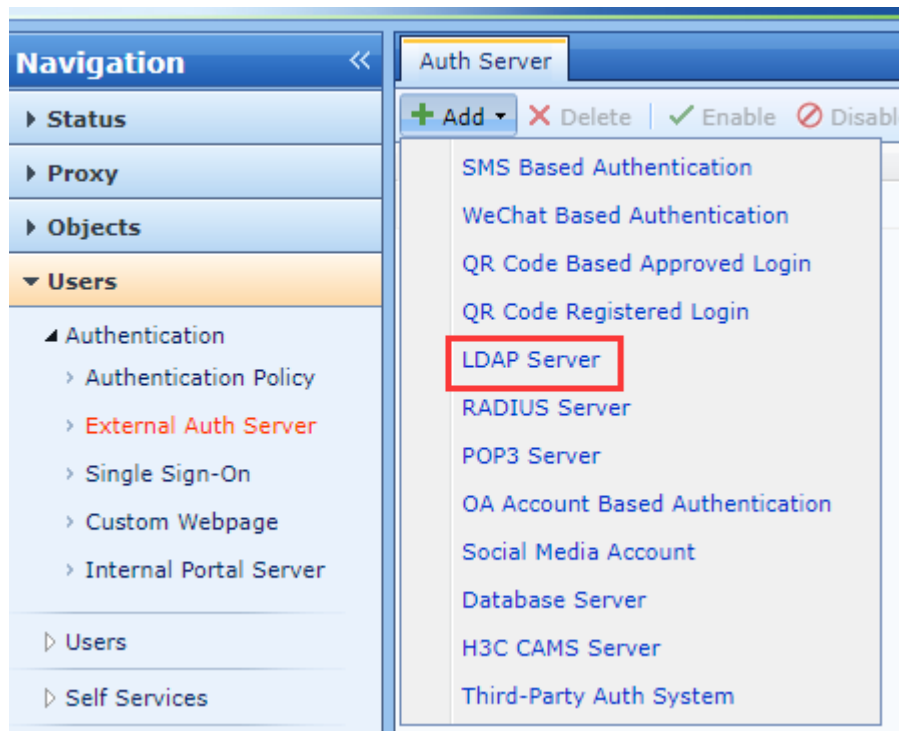
- ① PC masuk ke domain.
- ② Pengguna menelusuri website (Proses meliputi domain PC mengalihkan untuk mengunjungi Sangfor IAM resource, memicu autentikasi kerberos, domain SSO autentikasi dan semua proses transparan untuk pengguna akhir).

Catatan: Jika server signing requirement diaktifkan di AD Domain, koneksi enkripsi perlu diaktifkan pada konfigurasi single sign-on, sebaliknya IWA single sign-on akan terpengaruh. [Lihat Lampiran B]

Bab 4 Konfigurasi

Konfigurasi di IAM pada dasarnya mencakup 3 langkah : add new LDAP server, add new authentication policy dan configure IWA domain SSO, seperti yang ditunjukkan di bawah ini:

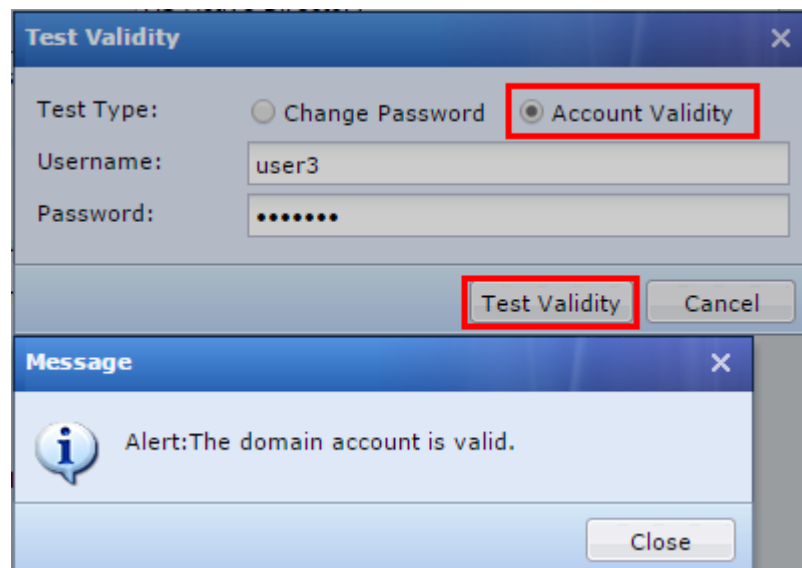
1. Add a new LDAP server.



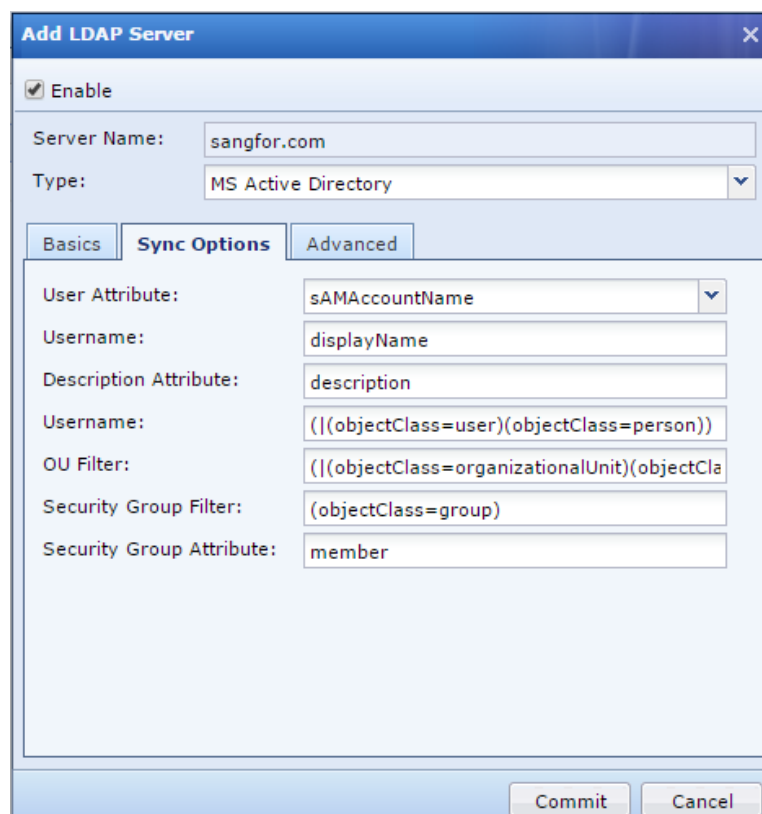
The 'Add LDAP Server' configuration dialog box is shown. The 'Enable' checkbox is checked. The 'Server Name' is 192.168.20.88, and the 'Type' is MS Active Directory. The 'Basics' tab is selected, showing fields for IP Address (192.168.20.89), Port (389), Timeout (5), Search (Anonymous), Admin DN (administrator@sccorp.local), and Admin Password. The 'Enable encryption' checkbox is checked, and the 'Encryption Method' is set to TLS. The 'Verify certificate' checkbox is unchecked. The 'BaseDN' is DC=SCCORP,DC=local. A 'Test Validity' button is present at the bottom.

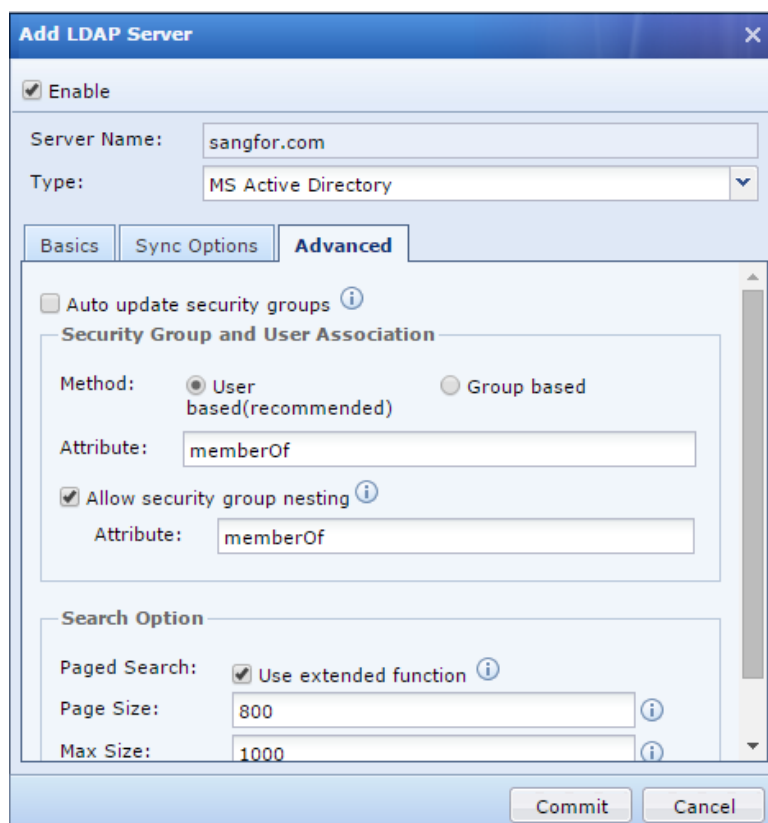
[Catatan]

- Halaman “Add LDAP Server” memiliki option “Test Validity”, hal ini dapat menguji domain account validity dan change domain account password melalui fungsi ini.

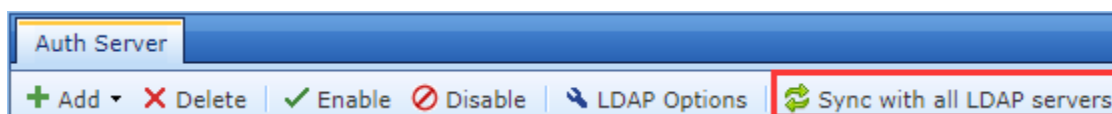


- b) Selain itu, halaman **"Add LDAP Server"** mengandung juga **"Sync Options"** dan **"Advanced"** dua tab, hanya perlu AD domain dan SUN domain **"Basics"** konfigurasi, **"Sync Options"** dan **"Advanced"** konfigurasi tetap ke pengaturan default. Jika domain lain tidak dapat ambil domain OU dengan menggunakan pengaturan default, dapat sesuaikan **"Sync Options"** untuk memecahkan masalah. Tab ditunjukkan pada gambar di bawah ini:





- c) Jika lingkungan pelanggan adalah independen domain, perlu untuk konfigurasi autentikasi port number 389 saat menambahkan LDAP server. Sebaliknya, jika domain berisi anak domain seperti ssl.sangfor.com, iam.sangfor.com untuk root domain sangfor.com, port number perlu dikonfigurasi ke 3268, IP address perlu dikonfigurasi ke root domain IP.
- d) Setelah konfigurasi domain server, domain OU secara otomatis akan melakukan sinkronisasi ke IAM lokal database, dan aksi ini akan dilakukan secara otomatis setiap 60 menit. Jika domain pengguna atau OU telah dimodifikasi dan perubahan perlu diterapkan ke IAM, klik pada **"Sync with all LDAP servers"** seperti yang ditunjukkan pada gambar di bawah ini :



- e) Jika AD domain tidak diaktifkan dengan **"LDAPS signing requirement service"**, **"LDAPS server certificate installation service"**, di IAM tidak perlu konfigurasi **"enable encryption"**.

Jika diperlukan:

[Enable encryption]: Pada bulan September 2019, Microsoft mengumumkan dalam buletin security [ADV190023 | Microsoft Guidance untuk mengaktifkan LDAP Channel Binding dan LDAP Signing] bahwa LDAP channel binding dan LDAP signing akan diaktifkan pada Active Directory server melalui metode security update (KB patch) pada pertengahan January 2020. Security Active Directory domain controllers dapat ditingkatkan secara signifikan dengan konfigurasi server untuk menolak Simple Authentication and Security Layer (SASL) LDAP binds yang tidak request signing (integrity verification) atau untuk menolak LDAP simple binds yang dilakukan pada koneksi clear text (non-SSL/TLS-encrypted). SASLs dapat

mencakup protokol Negotiate, Kerberos, NTLM, dan Digest . Untuk memenuhi kebutuhan security untuk Sangfor IAM, Sangfor IAM mendukung untuk enkripsi docking.

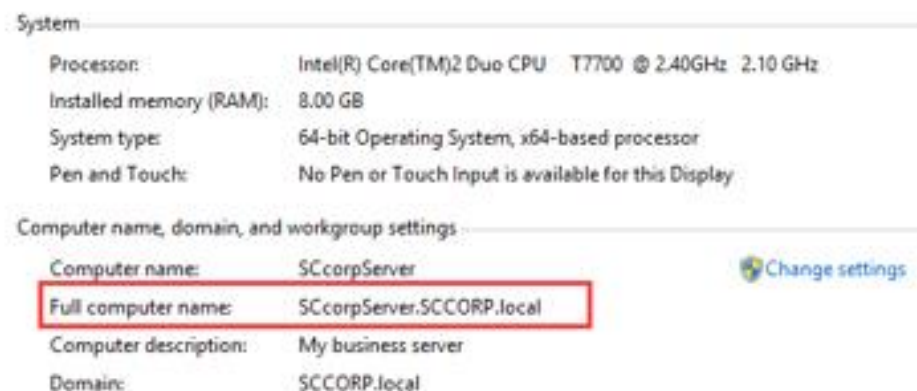
Konfigurasi resmi oleh Microsoft:

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

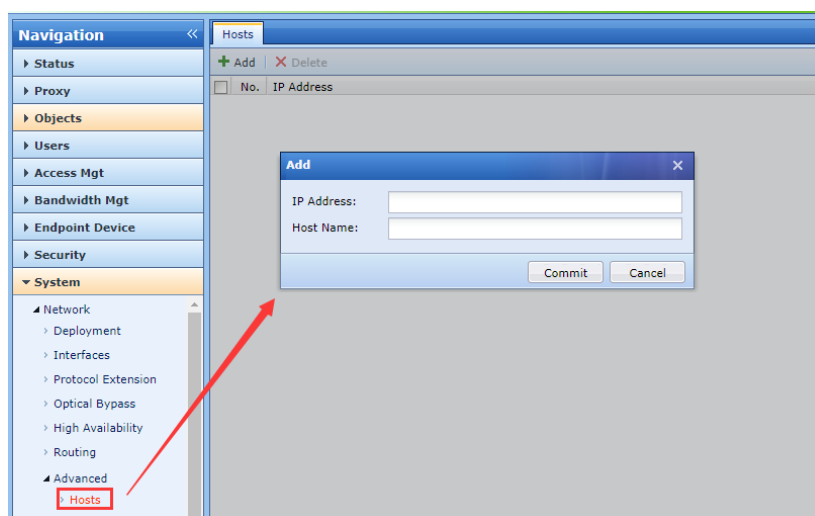
Metode Enkripsi: Jika AD domain server konfigurasi dengan [LDAPS signing requirement option], **disarankan untuk memilih TLS sebagai metode enkripsi** (Microsoft mendukung SSL dan TLS. Setelah AD domain mengaktifkan signature option, IAM hanya dapat terhubung ke AD melalui enkripsi. **Secara khusus, Windows 2000/2003/2008 tidak mendukung TLS enkripsi, hanya SSL enkripsi yang dapat digunakan**).

- Ketika enkripsi docking tidak diaktifkan, port default adalah 389.
- Jika enkripsi docking diaktifkan, ketika metode enkripsi adalah SSL, autentikasi port adalah 636.
- Jika enkripsi docking diaktifkan, ketika metode enkripsi adalah TLS, autentikasi port adalah 389.

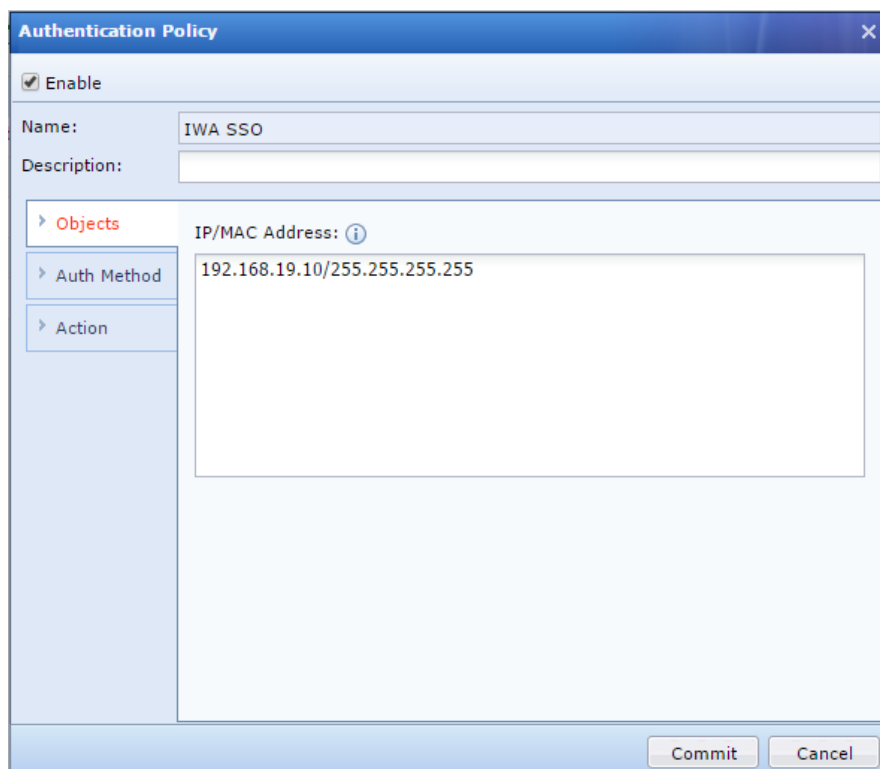
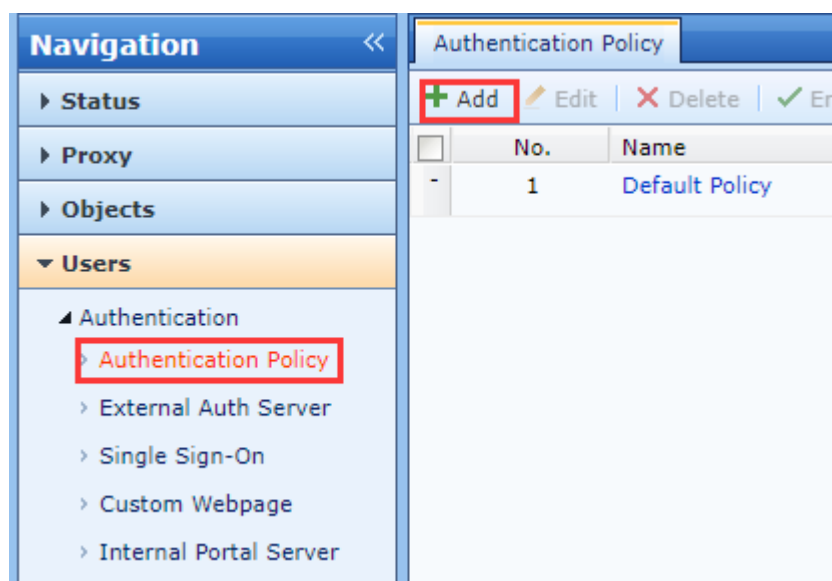
Verifikasi Sertifikat: Jika AD domain server dikonfigurasi dengan [LDAPS signing requirement option], Anda perlu konfigurasi item ini, isi domain name [AD domain server full computer name], dan import sertifikat.



Konfigurasi hosts: HOSTS menyelesaikan domain name menjadi IP dari AD domain server.



2. Add baru authentication policy.



Authentication Policy

☒ Enable

Name: IWA SSO

Description:

Objects

Auth Method

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

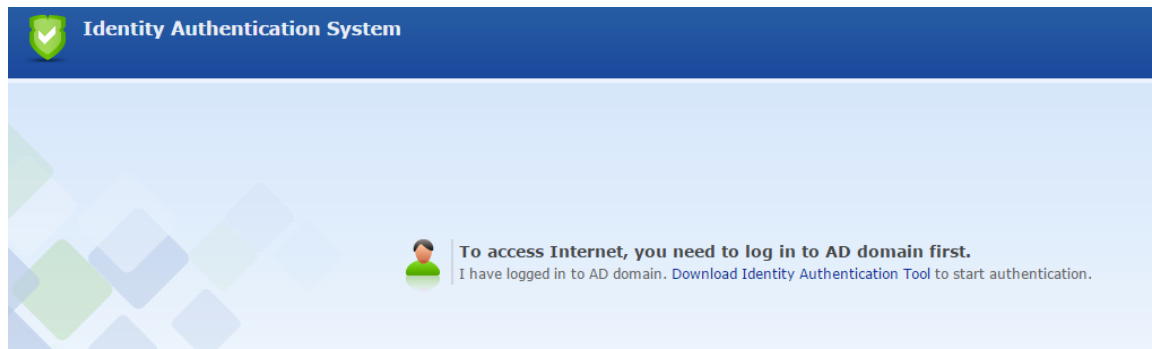
[Catatan]

① Ada empat metode penanganan untuk pengguna yang gagal autentikasi SSO seperti yang ditunjukkan pada “Auth Method” -> “For User Fails SSO” halaman; yang mana “Open authentication”, “Password based”, “Go to” dan “CAS server”. Metode ini dapat dikonfigurasi berdasarkan kebutuhan pengguna.

Jika admin mengizinkan akses internet untuk autentikasi SSO pengguna yang gagal, Pilih “Open authentication” untuk mencegah mengulang autentikasi lagi .

Jika persyaratannya adalah mencatat aktivitas untuk semua pengguna yang diautentikasi berdasarkan nama pengguna di domain, pilih “Password based” metode untuk memenuhi persyaratan.

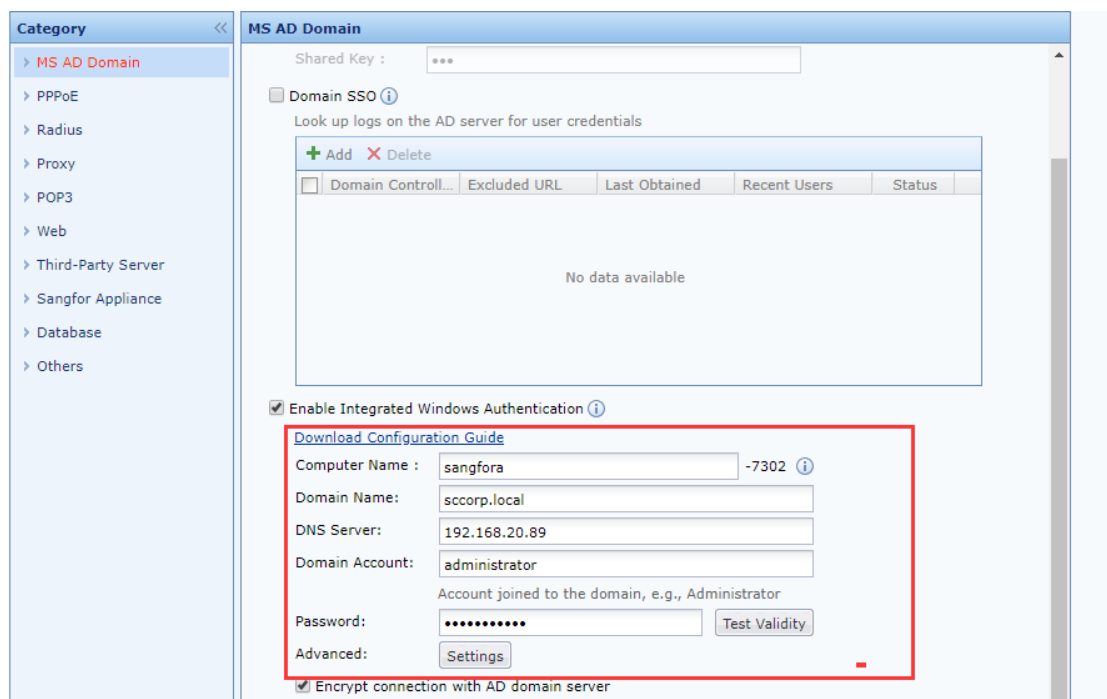
Selain itu, jika persyaratan pengguna adalah untuk mencatat aktivitas internet, dapat memilih juga option “Go to” dan pilih “predefined web page”. Domain pengguna yang gagal dalam autentikasi SSO akan dialihkan ke halaman web khusus seperti yang ditunjukkan di bawah ini untuk mengunduh Identity Authentication Tool dan jalankan untuk tujuan autentikasi.



Ketika pengguna memiliki persyaratan autentikasi yang ketat, yaitu, semua internet log yang dihasilkan oleh pengguna harus menjalani CAS authentication, kemudian pilih "CAS server". Jika single sign-on gagal, CAS third-party authentication digunakan.

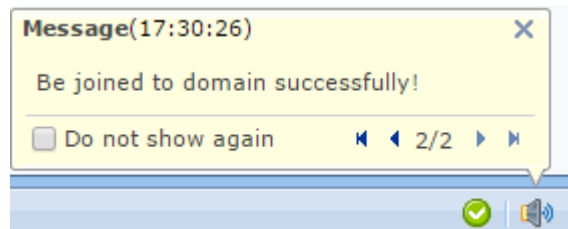
3. Konfigurasi IWA SSO option

Domain account yang digunakan untuk IAM untuk join harus memiliki hak istimewa untuk add workstation ke domain seperti administrator user account seperti yang ditunjukkan di bawah ini:



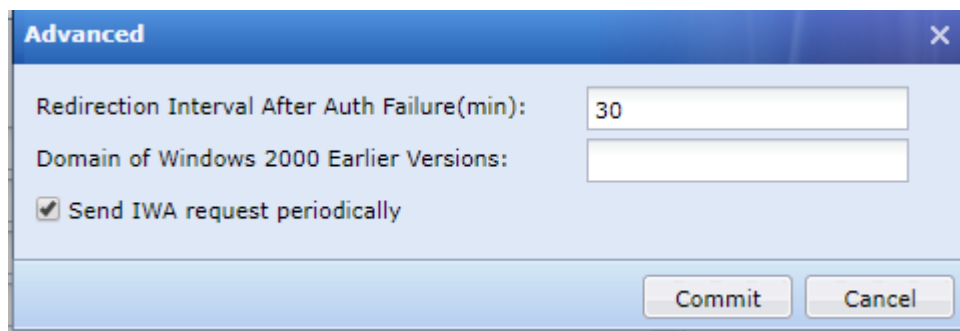
Catatan: Ketika "Server Signing Requirement" tidak diaktifkan di AD domain, ini tidak perlu diperiksa "encrypt connection with AD domain server".

Pesan yang di bawah ini ditampilkan setelah klik pada tombol button dan join domain berhasil:



[Catatan]

- a) Konfigurasi domain account di IAM IWA SSO harus memiliki hak istimewa untuk menambahkan workstation ke domain, merekomendasikan untuk menggunakan administrator account, regular domain account dapat menambahkan workstation ke domain tetapi hanya dapat add 10 times. Jika tidak dapat memberikan administrator account dan regular domain user account gagal untuk menambahkan, dapat membuat baru user account untuk pengujian.
- b) Kemudian Advanced settings dari konfigurasi IWA SSO ditampilkan di bawah ini:



Autentikasi IWA SSO memerlukan pengalihan http (proses ini transparan untuk pengguna), gambar di atas menunjukkan redirection interval after auth failure (default diatur ke 30 min), jika SSO gagal metode handling diatur ke "Open authentication", rekomendasi untuk mengubah nilainya menjadi 5min, jika tidak, simpan pengaturan default.

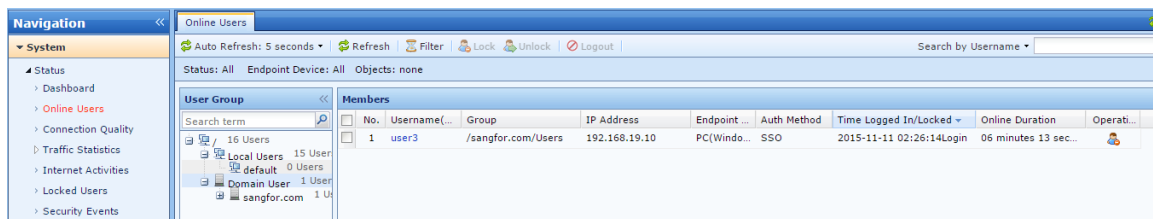
Untuk domain Windows 2000 dan sebelumnya : windows 2003 sampai versi terbaru, agar kompatibel dengan domain di windows 2000, perlu menentukan domain nama windows 2000 selama pengaturan domain. Jika domain name untuk Windows 2000 dan Windows 2003 berbeda, perlu menambahkan domain name ke dalam pengaturan "Domain of Windows 2000 Earlier Versions" seperti yang ditunjukkan pada gambar di atas. Jika Windows 2003 domain prefix sama dengan domain name di Windows 2000, maka tidak perlu menambahkan ke dalam konfigurasi.

Setelah konfigurasi selesai, lanjutkan ke bagian berikutnya untuk hasil pengujian.

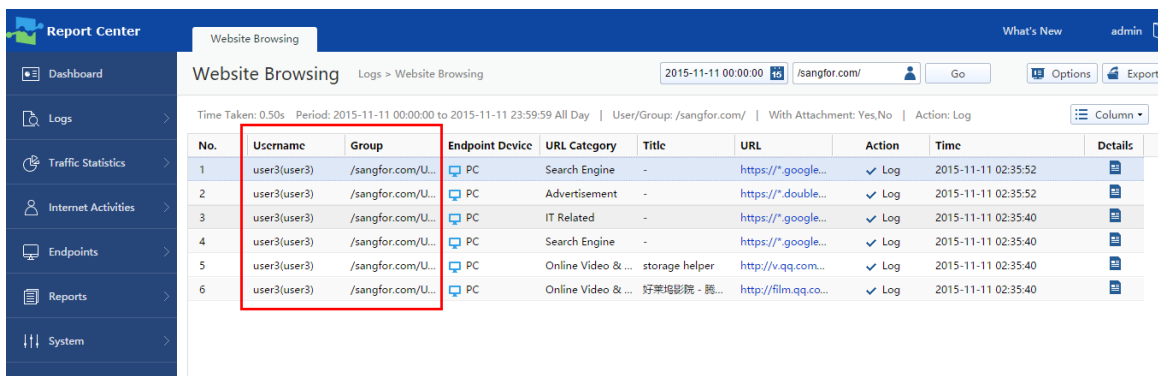
Bab 5 Hasil Pengujian

Hasilnya ditunjukkan seperti di bawah ini:

1. Ketika pengguna masuk ke domain dengan IWA SSO di IAM, browsing website tidak akan mengharuskan pengguna untuk melakukan autentikasi lagi. Rincian pengguna dapat dilihat dalam daftar pengguna Online IAM dan ini ditunjukkan sebagai SSO pada gambar di bawah ini:

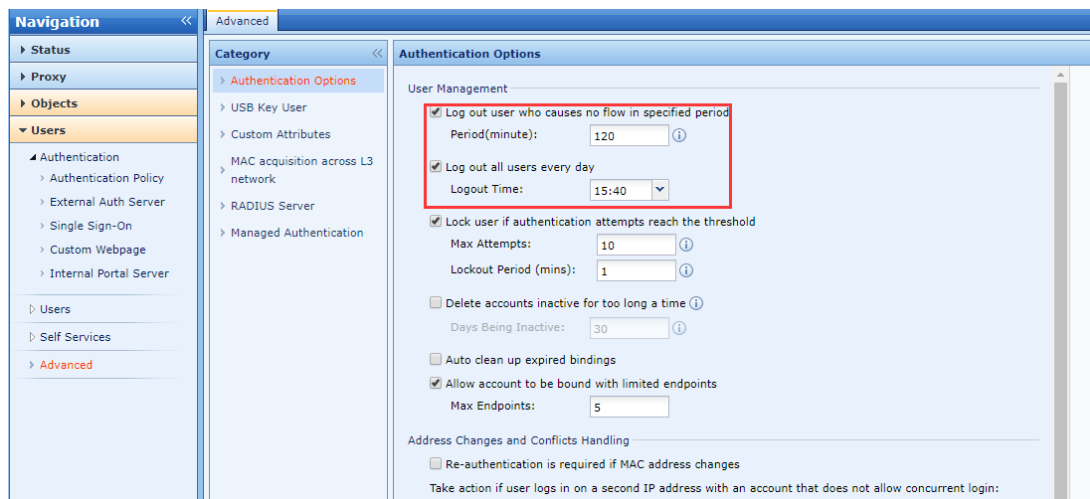


2. Setelah PC online melalui metode SSO, log di data center mencatat aktivitas pengguna di bawah domain user name mereka.

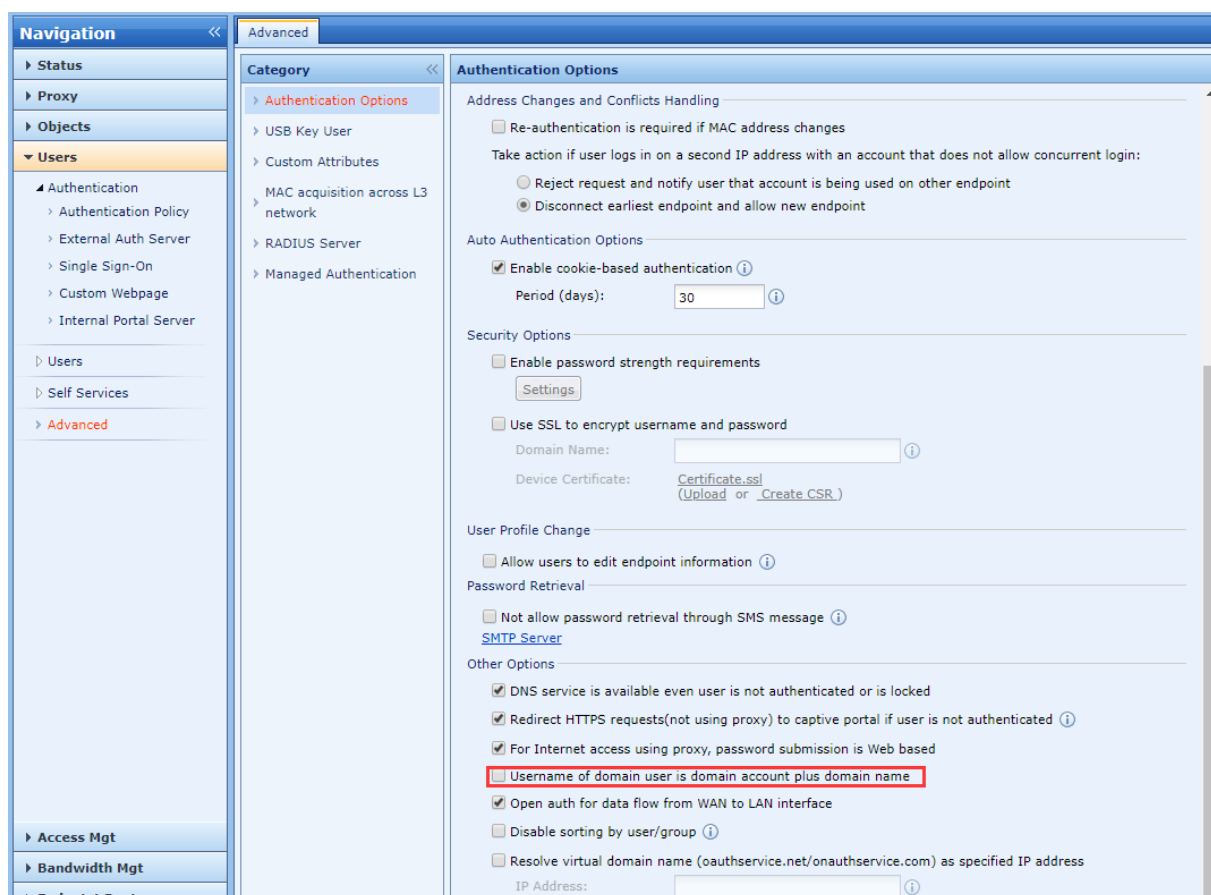


Bab 6 Tindakan Pencegahan

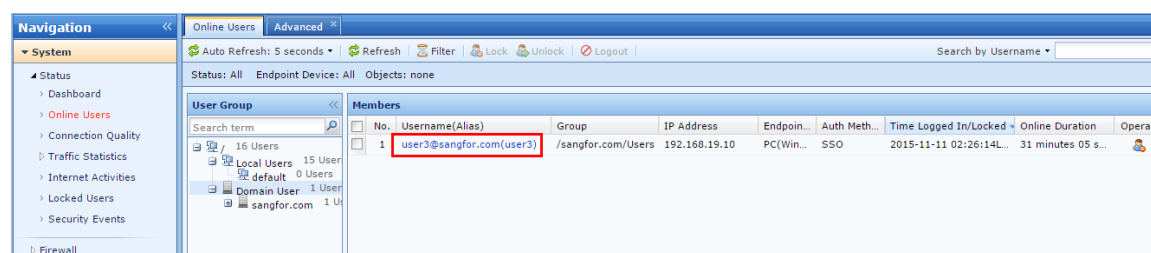
1. Autentikasi SSO IWA tidak mendukung online user logout di IAM ketika domain pengguna keluar dari PC mereka. Namun kita bisa menggunakan logout option di bawah "Authentication Options" halaman untuk log out dari pengguna tersebut.



2. Jika pengguna memiliki beberapa independent domains dan semua domains disinkronkan dengan IAM, konfigurasi option seperti yang ditunjukkan pada gambar di bawah untuk mengidentifikasi pengguna yang memiliki nama pengguna yang sama di domain yang berbeda.



Aktifkan option dan IAM akan secara otomatis menambahkan @domain name dalam daftar pengguna online seperti support@sangfor.com seperti yang ditunjukkan di bawah ini:



- Untuk autentikasi SSO, endpoint device harus menghasilkan traffic dan mengalir melalui IAM, maka hanya rincian pengguna (username, IP address) akan ditampilkan dalam daftar pengguna online. Proses IAM backend akan melakukan pemeriksaan untuk masing-masing 10 menit, jika tidak ada traffic yang terdeteksi, pengguna tidak akan ditambahkan ke daftar pengguna online.
- If AD server terletak di zona WAN dari IAM, dan domain PC tidak bisa masuk ke domain seperti biasa, maka IP address dari domain server perlu ditambahkan ke global excluded address di IAM karena PC traffics tidak dapat melewati IAM sebelum autentikasi.
- Dalam autentikasi IWA, setelah IAM bergabung domain, harus memastikan domain PC bisa ke telnet IAM PC name dengan port 80.
- Dengan signature service diaktifkan, IAM hanya dapat terhubung ke domain AD melalui enkripsi. Secara khusus, Windows 2000/2003/2008 tidak mendukung enkripsi TLS, dan hanya enkripsi SSL dapat digunakan. Windows Server 2008 R2 dan diatas mendukung kedua enkripsi TLS dan SSL.

Bab 7 Lampiran A: Panduan Konfigurasi LDAPS

7.1 Latar Belakang

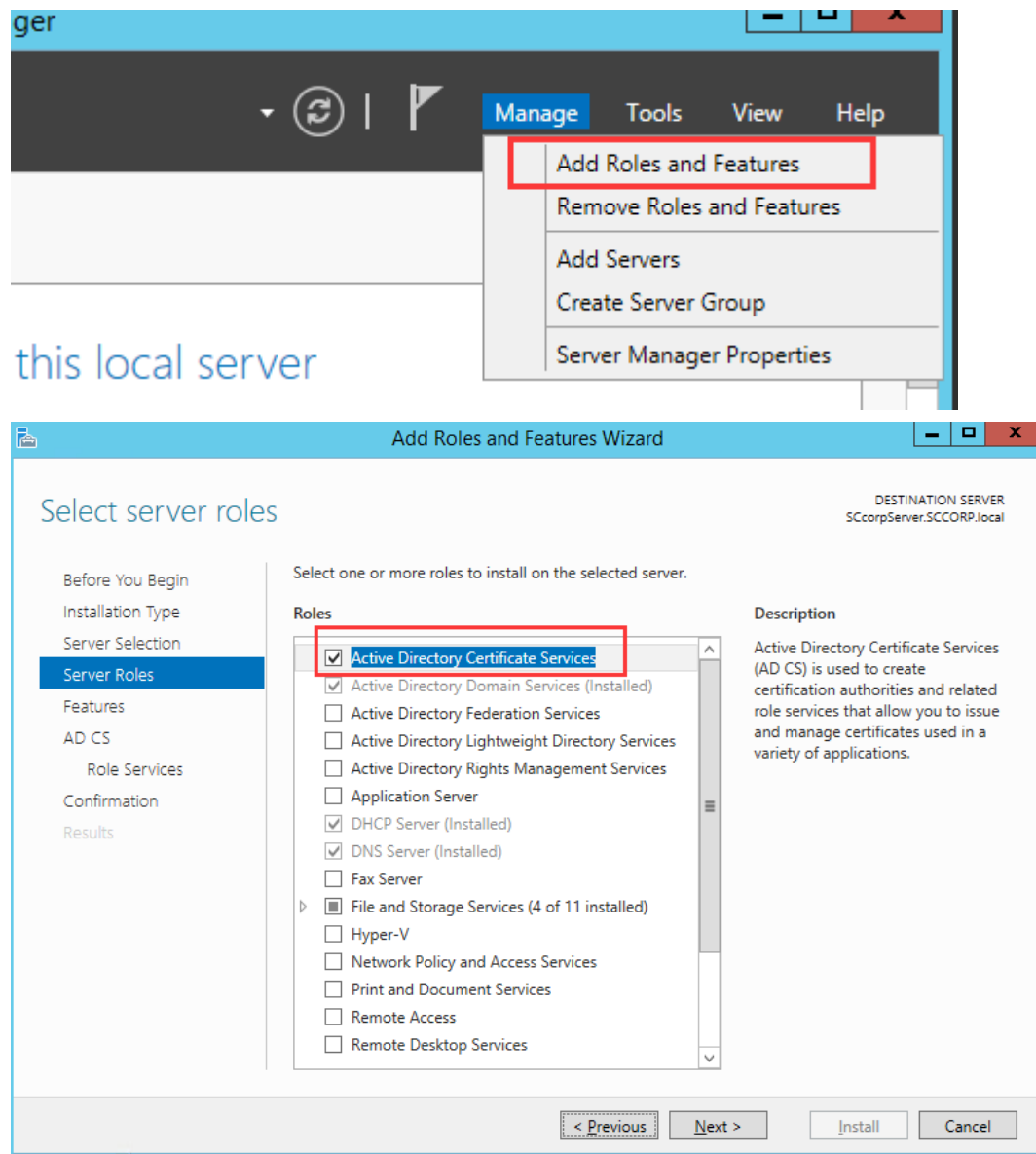
Pada bulan September 2019, Microsoft mengumumkan dalam buletin keamanan [ADV190023 | Microsoft Guidance for Enabling LDAP Channel Binding and LDAP Signing] bahwa LDAP channel binding dan LDAP signing akan diaktifkan di Active Directory server melalui metode security update (KB patch) pada pertengahan January 2020.

Security dari Active Directory domain controllers dapat ditingkatkan secara signifikan dengan mengkonfigurasi server untuk menolak Simple Authentication and Security Layer (SASL) LDAP binds yang tidak meminta signing (integrity verification) atau untuk menolak LDAP simple binds yang dilakukan pada clear text koneksi yang jelas (non-SSL/TLS-encrypted). SASLs termasuk protokol seperti Negotiate, Kerberos, NTLM, dan protokol Digest.

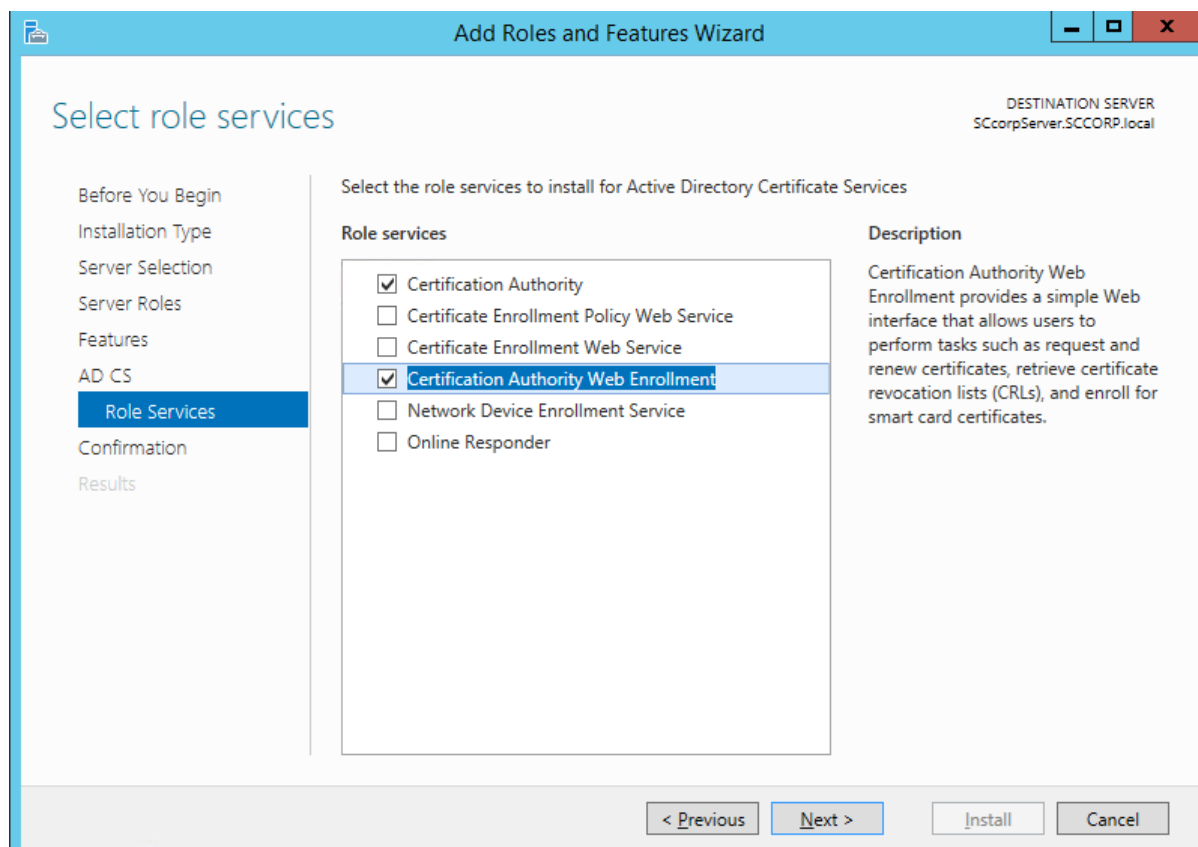
7.2 Konfigurasi dari Instalasi Sertifikat Server

Setelah menginstal sertifikat service, sertifikat server root dapat diekspor untuk verifikasi sertifikat klien untuk meningkatkan security. Untuk cara install sertifikat service di server Active Directory server, lihat ke tutorial berikut:

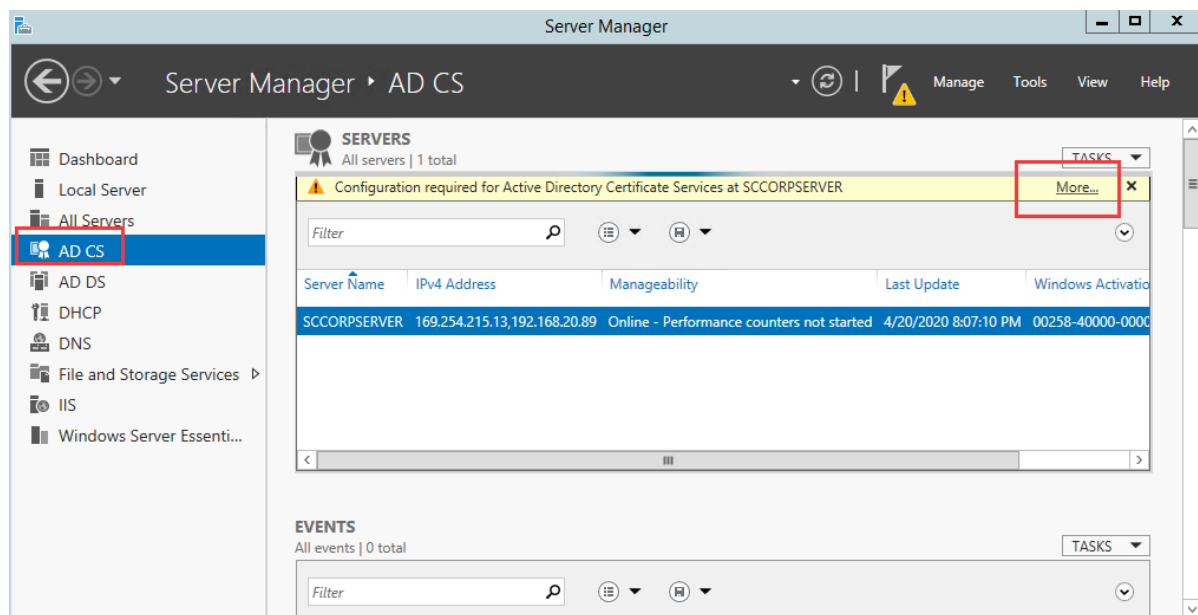
Buka Server Manager, klik kanan add Roles and Features (using 2012 R2 to test), instal Active Directory Certificate Services:

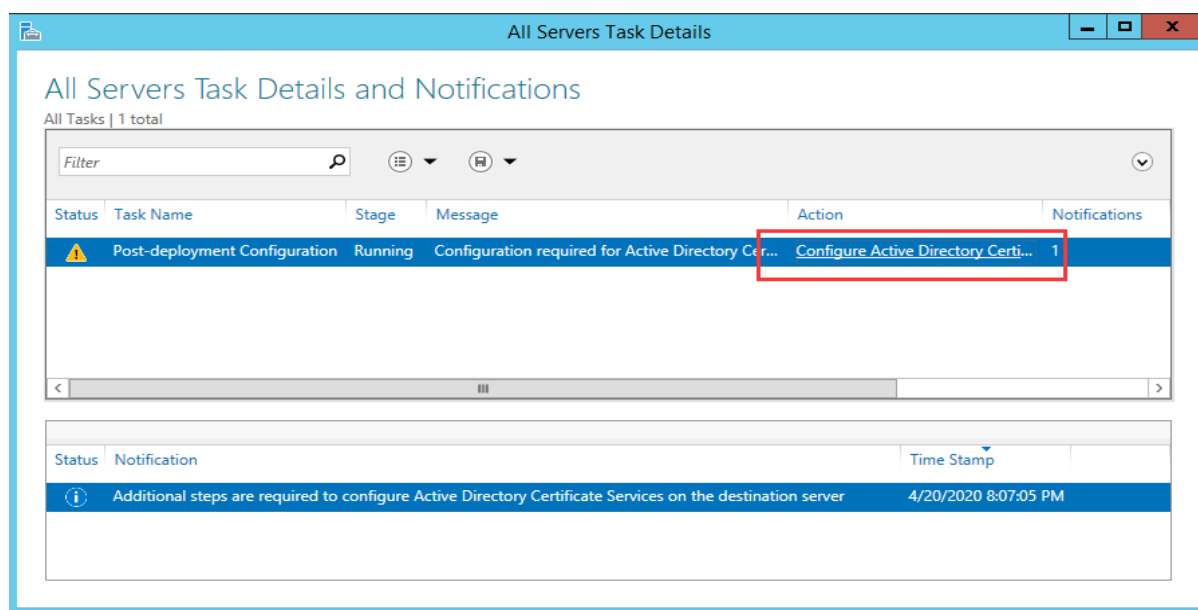


Pilih Certificate Authority dan Certificate Authority Web Enrollment:



Pergi ke AD CS, pilih lebih banyak dan klik pada Configure Active Directory Certification:





Pilih Enterprise CA:

The screenshot shows the 'AD CS Configuration' window 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: 'local Administrators group' (Standalone certification authority, Certification Authority Web Enrollment, Online Responder) and '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. At the bottom are buttons for '< Previous', 'Next >', 'Configure', and 'Cancel'. The 'DESTINATION SERVER' is 'SCcorpServer.SCCORP.local'.

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' window 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 shows a list of 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). At the bottom are buttons for '< Previous', 'Next >', 'Configure', and 'Cancel'. The 'DESTINATION SERVER' is 'SCcorpServer.SCCORP.local'.

AD CS Configuration

DESTINATION SERVER
SCcorpServer.SCCORP.local

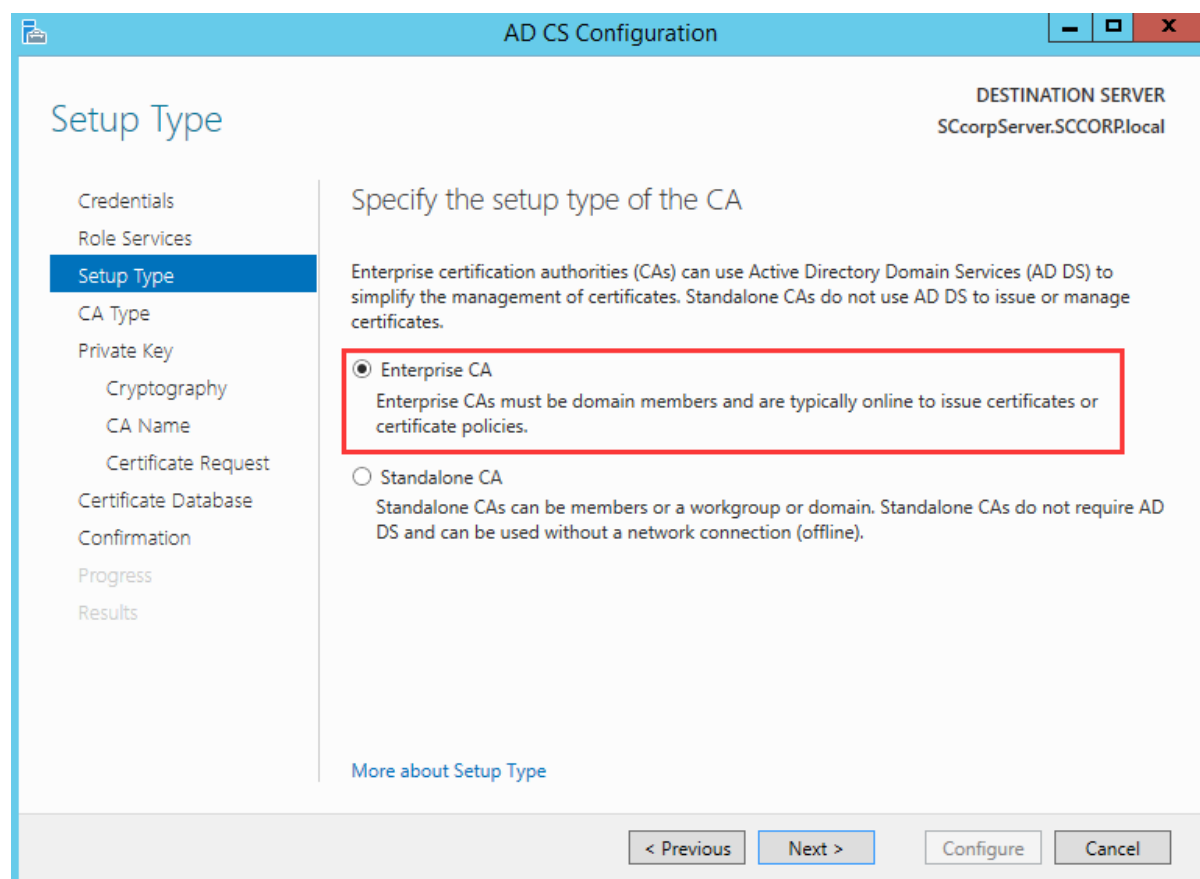
Role Services

Select Role Services to configure

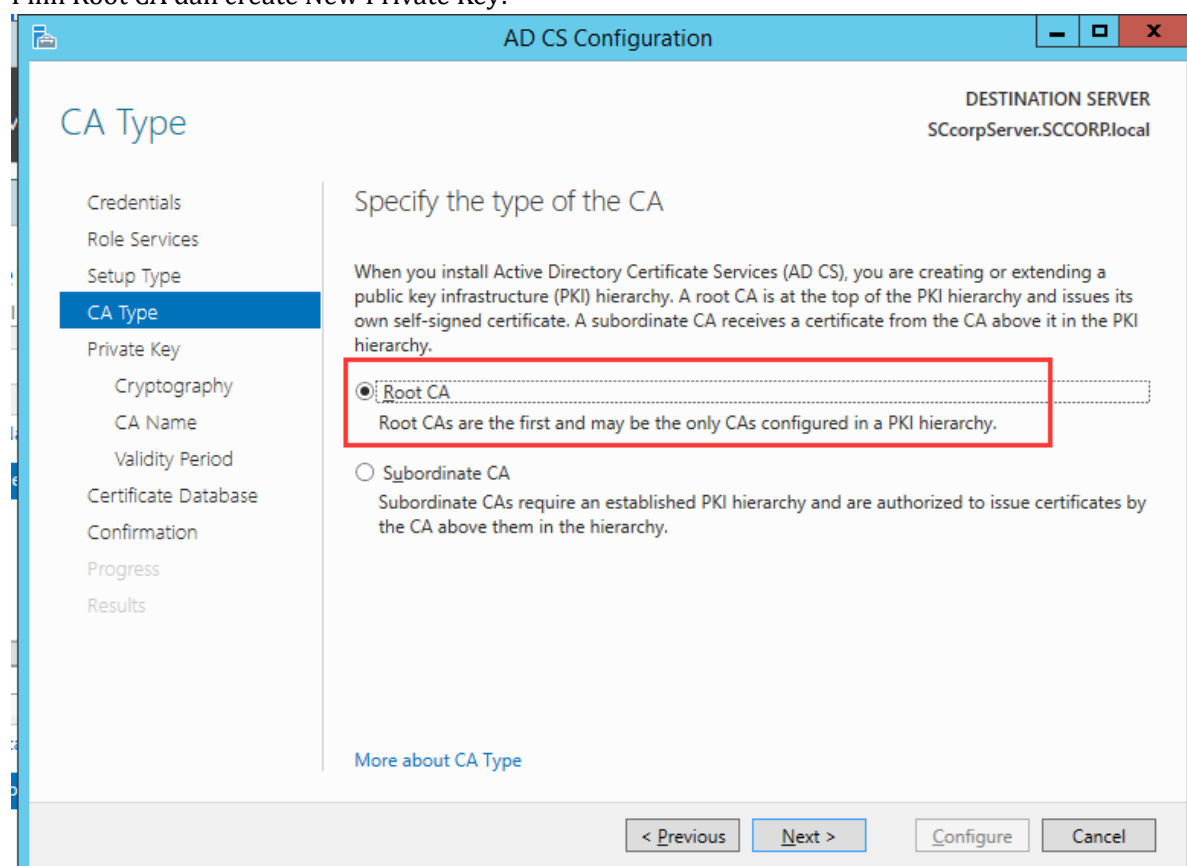
- ☒ Certification Authority
- ☒ Certification Authority Web Enrollment
- ☐ Online Responder
- ☐ Network Device Enrollment Service
- ☐ Certificate Enrollment Web Service
- ☐ Certificate Enrollment Policy Web Service

[More about AD CS Server Roles](#)

< Previous Next > Configure Cancel



Pilih Root CA dan create New Private Key:



The screenshot shows the 'Private Key' step of the AD CS Configuration wizard. The title bar is 'AD CS Configuration' with standard window controls. The left sidebar lists steps: Credentials, Role Services, Setup Type, CA Type, Private Key (selected), Cryptography, CA Name, Validity Period, Certificate Database, Confirmation, Progress, and Results. The main area is titled 'Specify the type of the private key'. It explains that a CA must have a private key to generate and issue certificates. There are three radio button options: 'Create a new private key' (selected), 'Use existing private key', and 'Select a certificate and use its associated private key'. The 'Create a new private key' option has a sub-note: 'Use this option if you do not have a private key or want to create a new private key.' The 'Use existing private key' option has a sub-note: 'Use this option to ensure continuity with previously issued certificates when reinstalling a CA.' The 'Select a certificate and use its associated private key' option has a sub-note: '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.' The 'Select an existing private key on this computer' option has a sub-note: 'Select this option if you have retained private keys from a previous installation or want to use a private key from an alternate source.' At the bottom right, there is a 'More about Private Key' link. The bottom navigation bar contains buttons: '< Previous', 'Next >', 'Configure', and 'Cancel'. The 'DESTINATION SERVER' is listed 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

Mengatur validity period:

The screenshot shows the 'Validity Period' step of the AD CS Configuration wizard. The title bar is 'AD CS Configuration' with standard window controls. The left sidebar lists steps: Credentials, Role Services, Setup Type, CA Type, Private Key, Cryptography, CA Name, Validity Period (selected), Certificate Database, Confirmation, Progress, and Results. The main area is titled 'Specify the validity period'. It asks to 'Select the validity period for the certificate generated for this certification authority (CA):'. There is a text input field containing '100' and a dropdown menu set to 'Years'. Below this, it shows '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 right, there is a 'More about Validity Period' link. The bottom navigation bar contains buttons: '< Previous', 'Next >', 'Configure', and 'Cancel'. The 'DESTINATION SERVER' is listed 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

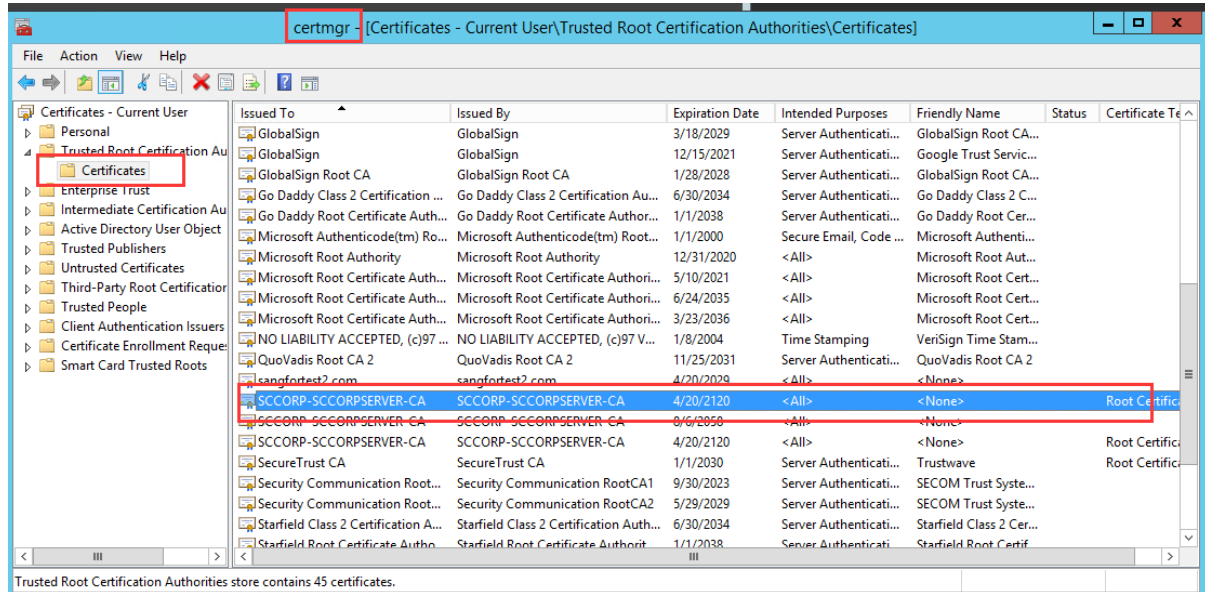
Specify the database location:

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 fields 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.

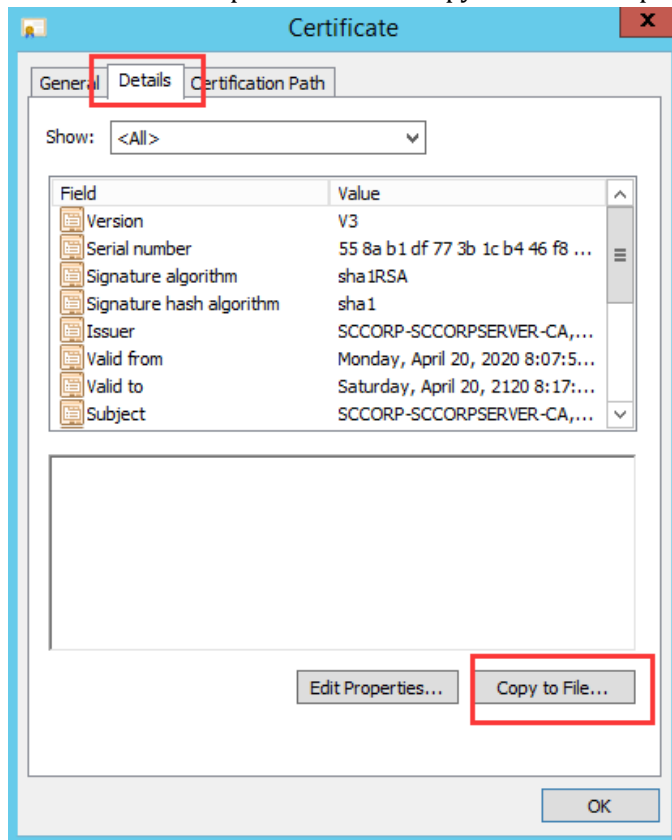
Instalasi selesai:

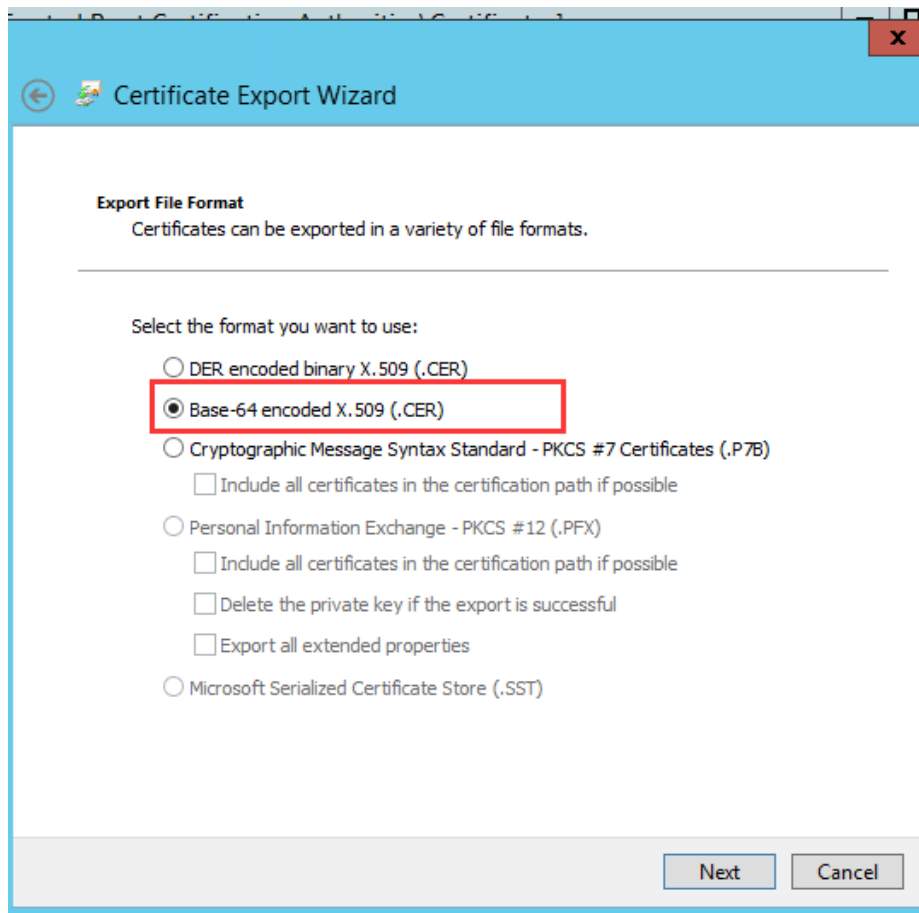
The screenshot shows the 'AD CS Configuration' window with the 'Results' step selected in the left-hand navigation pane. The main area is titled 'Results'. It displays a summary of the configuration: 'The following roles, role services, or features were configured:'. Under the heading 'Active Directory Certificate Services', there are two items: '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 visible at the top right.

Pergi ke certmgr.msc:



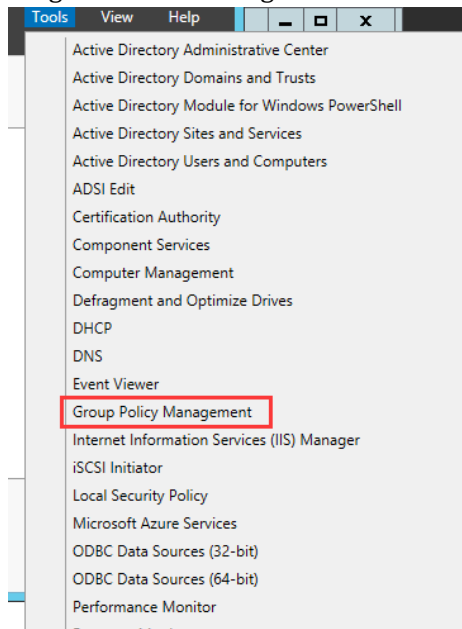
Buka cert dan klik pada Details -> Copy to File dan export as Base-64 dengan .cer format:



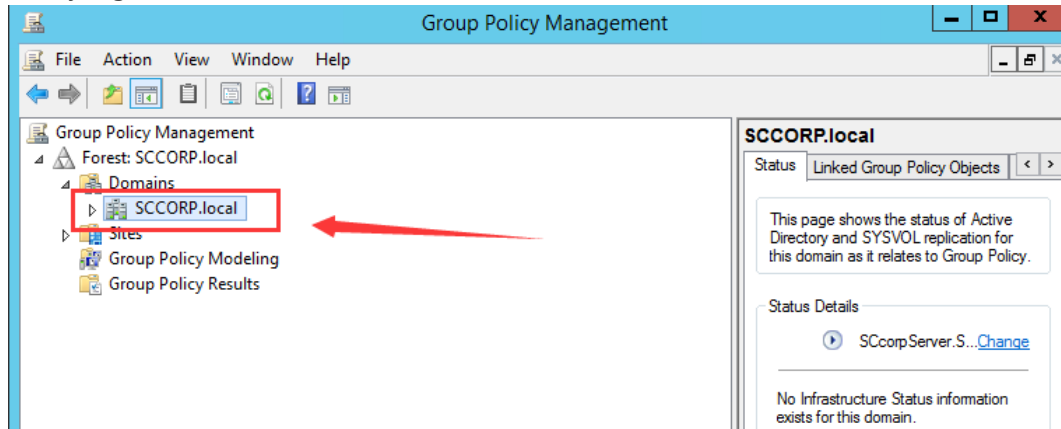


7.3 Konfigurasi dari LDAPS Server Signing

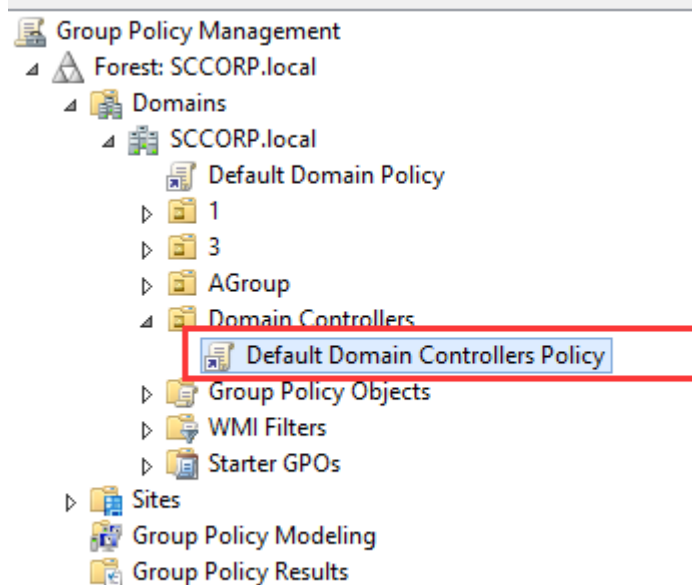
Pergi ke Server Manager ->Tools -> Klik Group Policy Management:



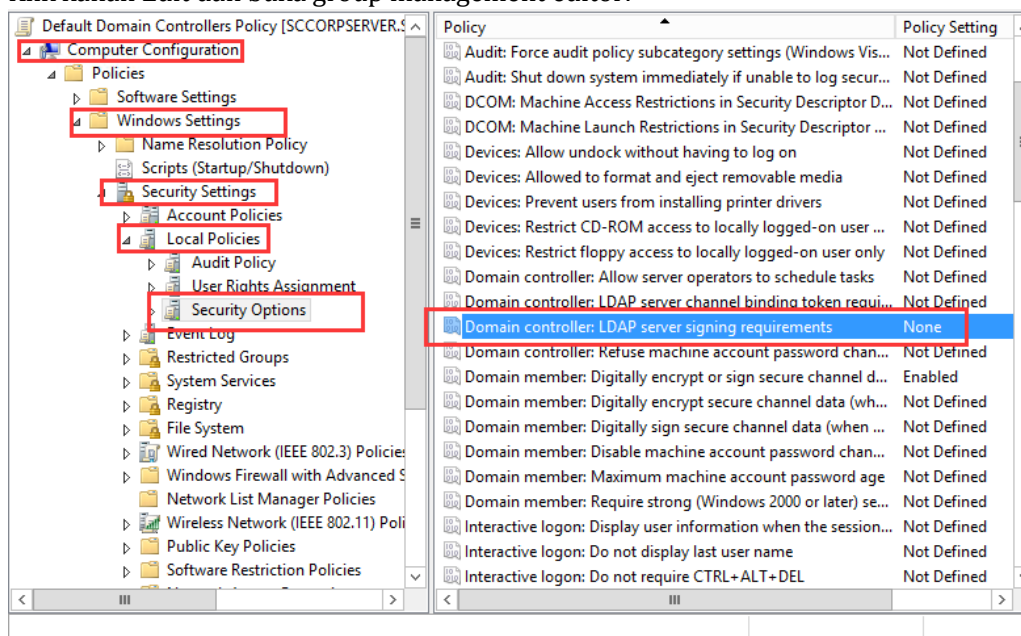
Pilih yang benar Domain name dan Extend it.



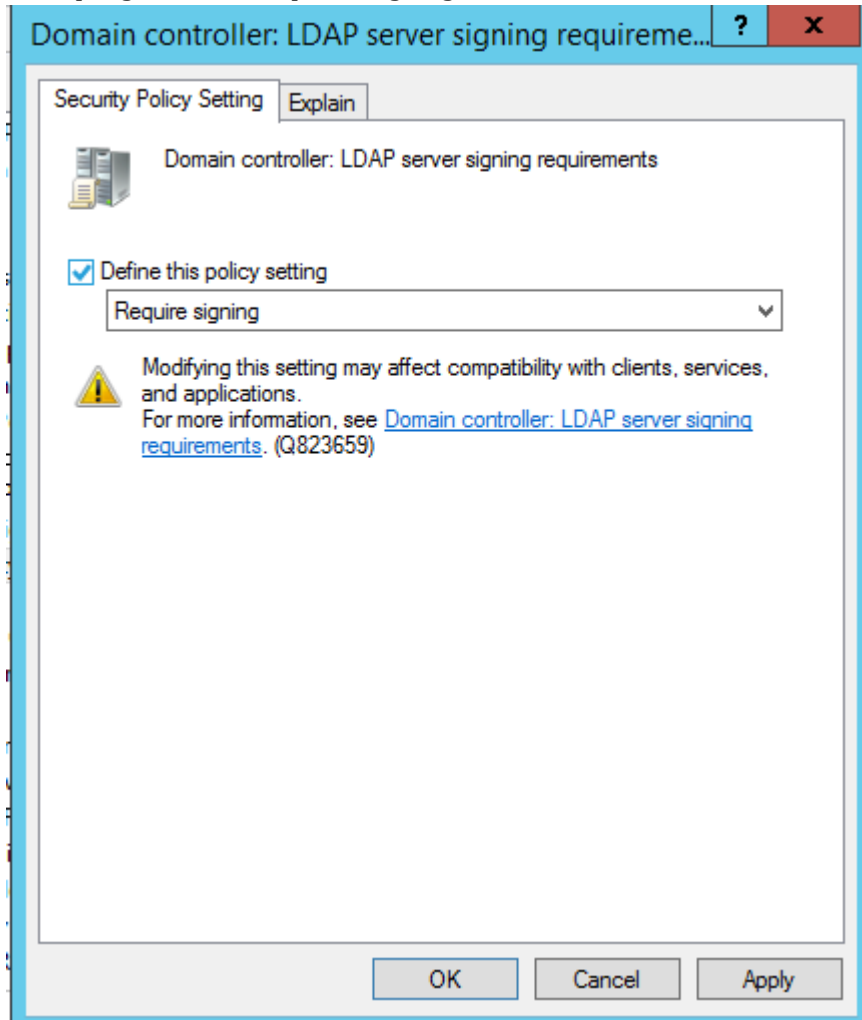
Pilih domain controller -> Pilih Default Domain controller Policy:



Klik kanan Edit dan buka group management editor:



Ubah pengaturan ke Required signing.



Setelah konfigurasi, CMD jalankan gpupdate /force untuk push 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>
```

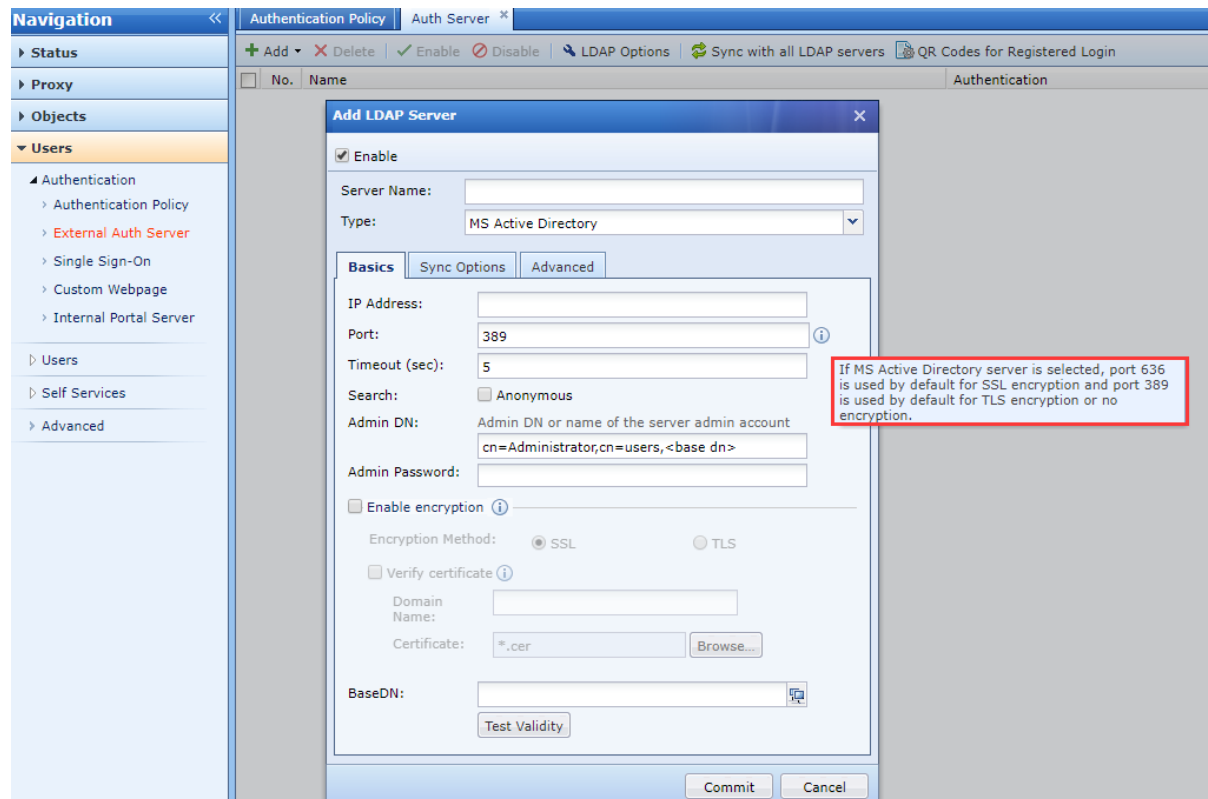
7.4 Konfigurasi AD pada IAM

Diatas adalah tutorial konfigurasi pada AD domain. Bagian ini menjelaskan konfigurasi AD domain server di IAM:

7.4.1 Deskripsi Autentikasi Port

Seperti yang ditunjukkan pada gambar, LDAP server dikonfigurasi di server autentikasi eksternal untuk terhubung dengan Microsoft AD domain:

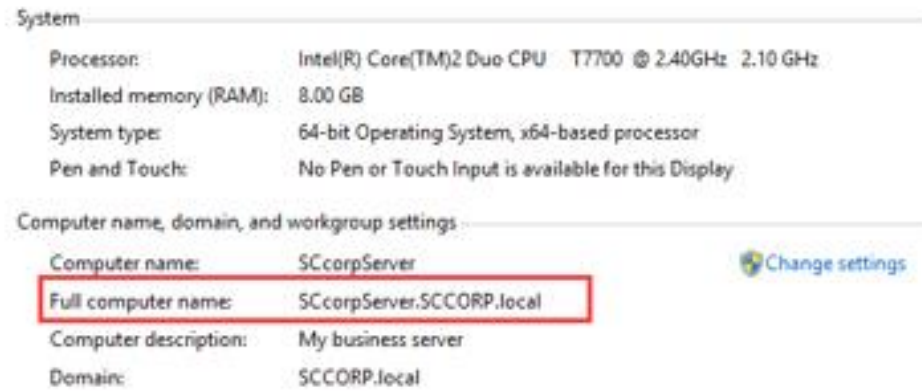
- Ketika encryption tidak diaktifkan, default port 389.
- Jika encryption diaktifkan, ketika metode encryption adalah SSL, autentikasi port 636.
- Jika encryption diaktifkan, ketika metode encryption adalah TLS, autentikasi port 389.



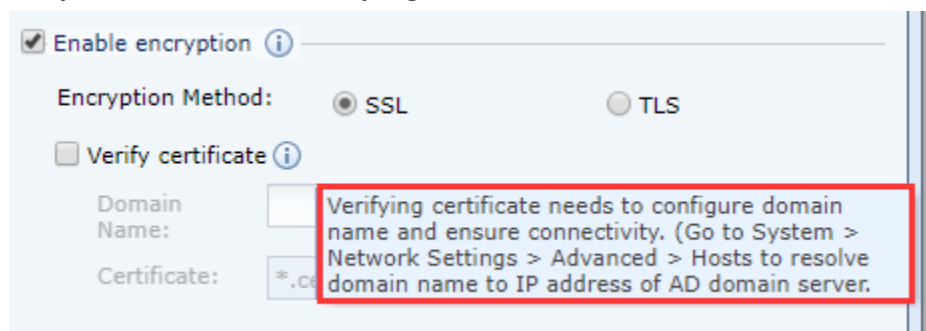
7.4.2 Enable Encryption

Seperti yang ditunjukkan pada gambar di bawah ini:

- The LDAP server dapat dikonfigurasi untuk tidak enable encryption. Dalam skenario ini, LDAP server signing requirement tidak diaktifkan di Microsoft AD domain.
- Jika AD domain telah dikonfigurasi untuk mengaktifkan LDAP server signing requirement, maka encryption harus diaktifkan di sini. The encryption metode encryption dapat dipilih sendiri, dan autentikasi port dapat dimodifikasi sesuai dengan metode encryption yang dipilih seperti yang dijelaskan di atas.
- Verify certificate function dapat dimatikan, and ini tidak akan mempengaruhi koneksi dengan AD domain dengan server signing requirement diaktifkan.
- Jika verify certificate function diaktifkan, Anda perlu konfigurasi domain name dan import certificate file:
 - Konfigurasi domain name perlu dikonfigurasi sebagai full computer name dari AD domain server: seperti yang ditunjukkan di bawah ini, Anda dapat masuk ke AD domain server untuk memperoleh field ini, seperti yang ditunjukkan pada gambar berikut:



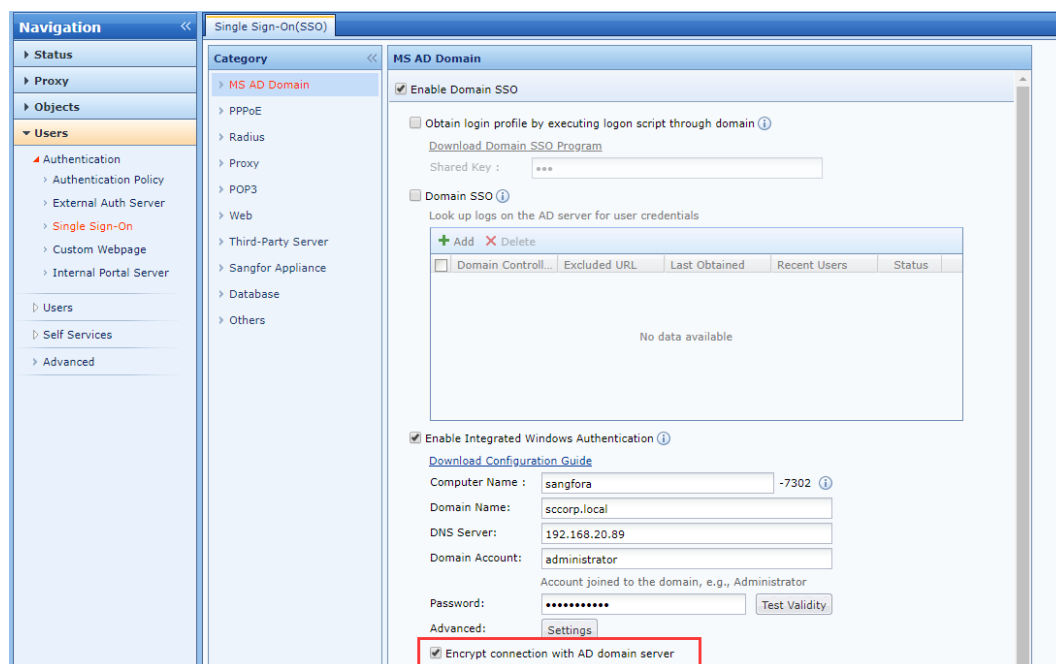
- Setelah domain name di konfigurasi, Anda perlu menambahkan host rule untuk menyelesaikan domain name yang diisi ke IP address dari AD domain server:



- Import sertifikat. Sertifikat harus berupa Base64 encoded .cer format certificate yang diekspor dari root certificate file di AD domain server. Hal ini dijelaskan dalam [Configuration of Server Certification Installation] bagian dan tidak akan diulang disini.

7.5 Konfigurasi IWA SSO

IWA single sign-on function fungsi akan terpenuhi oleh **server signing requirement** diaktifkan di AD domain. Jika server signing requirement diaktifkan pada AD domain, Anda harus mengaktifkan encrypt connection pada lokasi IWA single sign-on:





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