SANGFOR

IAM

Password-based autentikasi dengan AD

Versi 12.0.42

Catatan Perubahan

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

Daftar Isi

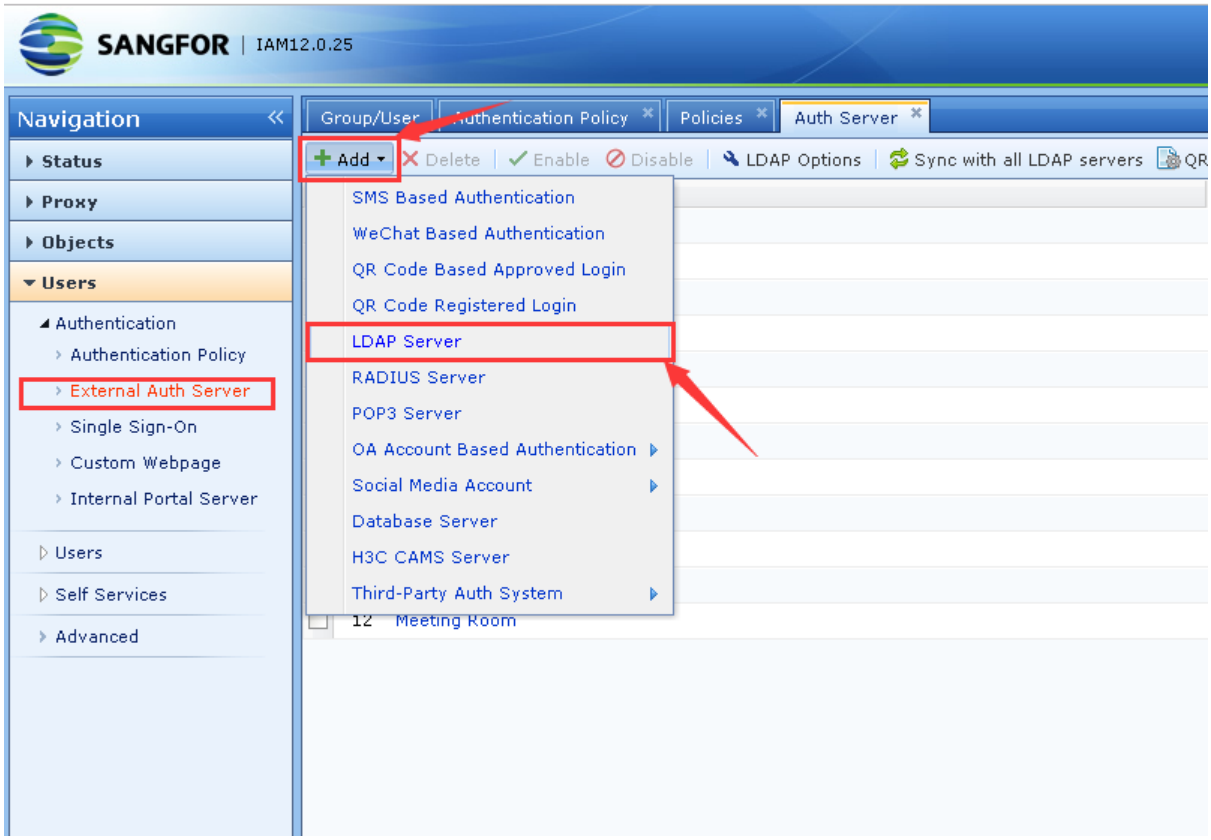
Bab 1 Persyaratan Isi

1. Perangkat IAM (versi 12.0.42 atau lebih tinggi), PC, dan AD domain server.
2. Terapkan lingkungan network , pastikan semua perangkat dan AD domain server dapat terhubung ke IAM.

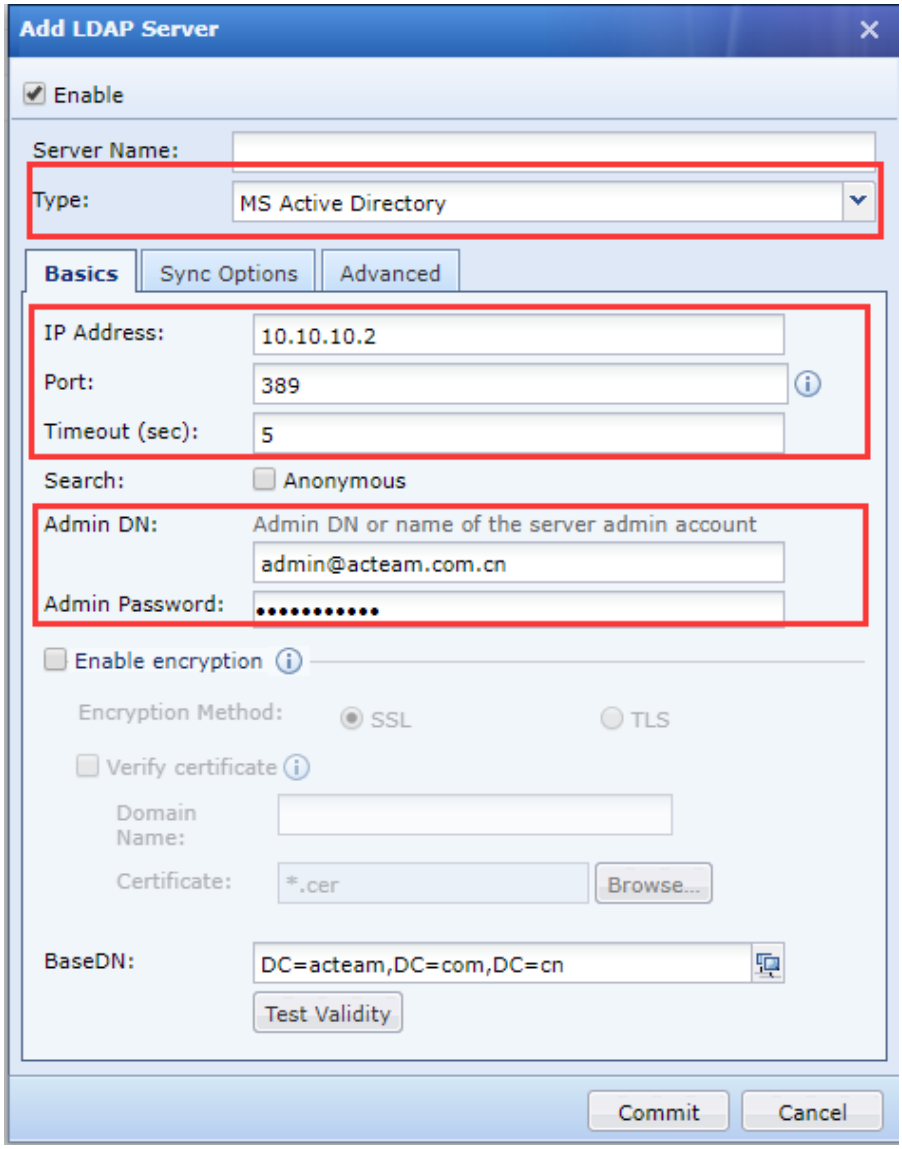
Bab 2 Konfigurasi dan Tangkapan Layar

2.1 Konfigurasi LDAP Server

1. Edit **Users > External Auth Server > Add > LDAP Server.**



2. Konfigurasi informasi LDAP server.



[IP Address]: IP address dari LDAP server.

[Authentication port]: Port yang terhubung ke LDAP server, misalnya, AD domain adalah 389.

[Timeout]: Mengatur periode timeout dari permintaan autentikasi. Setelah sistem meneruskan permintaan autentikasi ke LDAP server, jika tidak ada tanggapan setelah waktu ini, autentikasi dianggap tidak valid. Jika network antara perangkat dan LDAP server lambat, Anda dapat mencoba mengatur waktu tenggang menjadi lebih besar (misalnya, 10 detik).

[Search]: Option ini tersedia ketika LDAP server mendukung anonymous search.

[Admin DN]: Pengguna akun yang digunakan untuk membuat kueri dan menyinkronkan LDAP server; misalnya, akunnya adalah: administrator, nama domainnya adalah sangfor.com, maka formatnya adalah: username@domain, administrator@sangfor.com.cn

[Admin Password]: Password yang sesuai dengan pengguna yang digunakan untuk mengikat server.

[BaseDN]: Spesifikasikan titik awal dari domain search path, yang menentukan ruang lingkup

efektif dari LDAP rule. Jika pengguna berada di luar yang ditentukan BaseDN, pengguna tidak dapat diautentikasi oleh external server, dan konfigurasi policy tidak akan berlaku untuk pengguna. Oleh karena itu, Anda dapat menggunakan BaseDN untuk membagi area administrator yang berbeda.

[Enable encryption]: Pada bulan September 2019, Microsoft mengumumkan di buletin security. [ADV190023 | Microsoft Guidance for Enabling LDAP Channel Binding and LDAP Signing] bahwa LDAP channel binding dan LDAP signing akan diaktifkan pada Active Directory server melalui metode pembaharuan security (KB patch) pada pertengahan Januari 2020. Security Active Directory domain controllers dapat secara signifikan ditingkatkan dengan konfigurasi server untuk menolak Simple Authentication dan Security Layer (SASL) LDAP binds yang tidak request signing (integrity verification) atau 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.

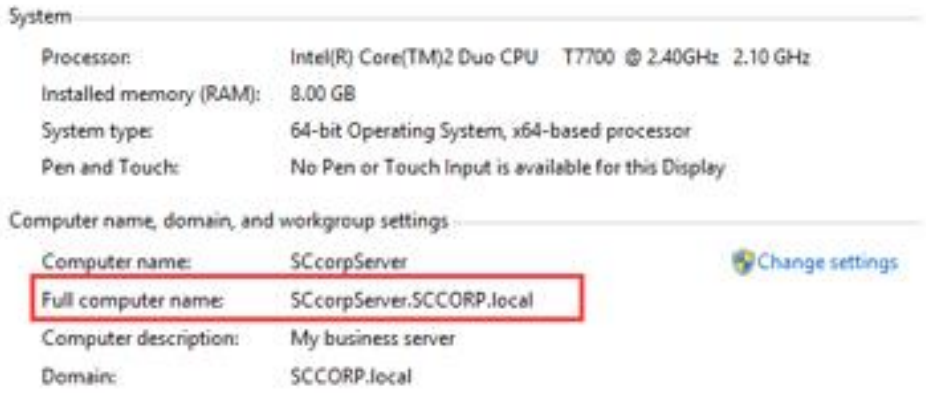
Konfigurasi resmi oleh Microsoft：

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

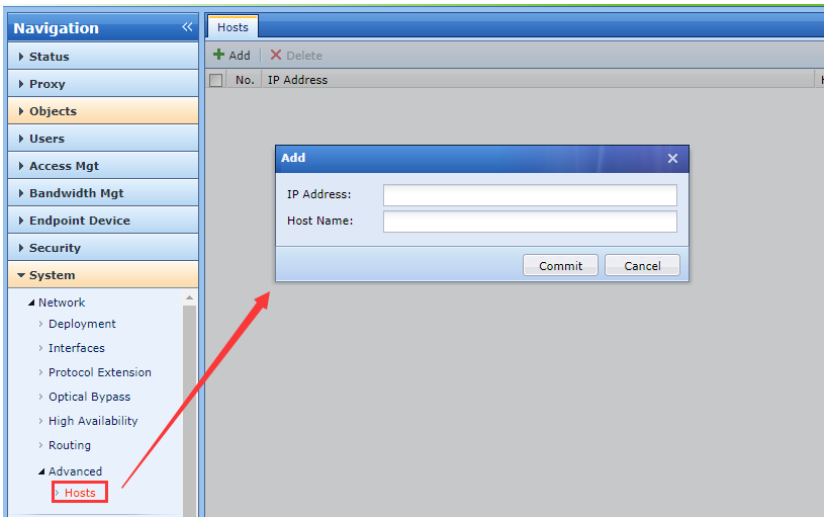
Metode Enkripsi: Jika AD domain server konfigurasi dengan [LDAPS signing requirement option], disarankan untuk memilih TLS sebagai metode enkripsi (Microsoft mendukung SSL dan TLS. Setelah AD domain mengaktifkan signature option, IAM hanya dapat terhubung ke AD melalui enkripsi. Secara khusus, Windows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

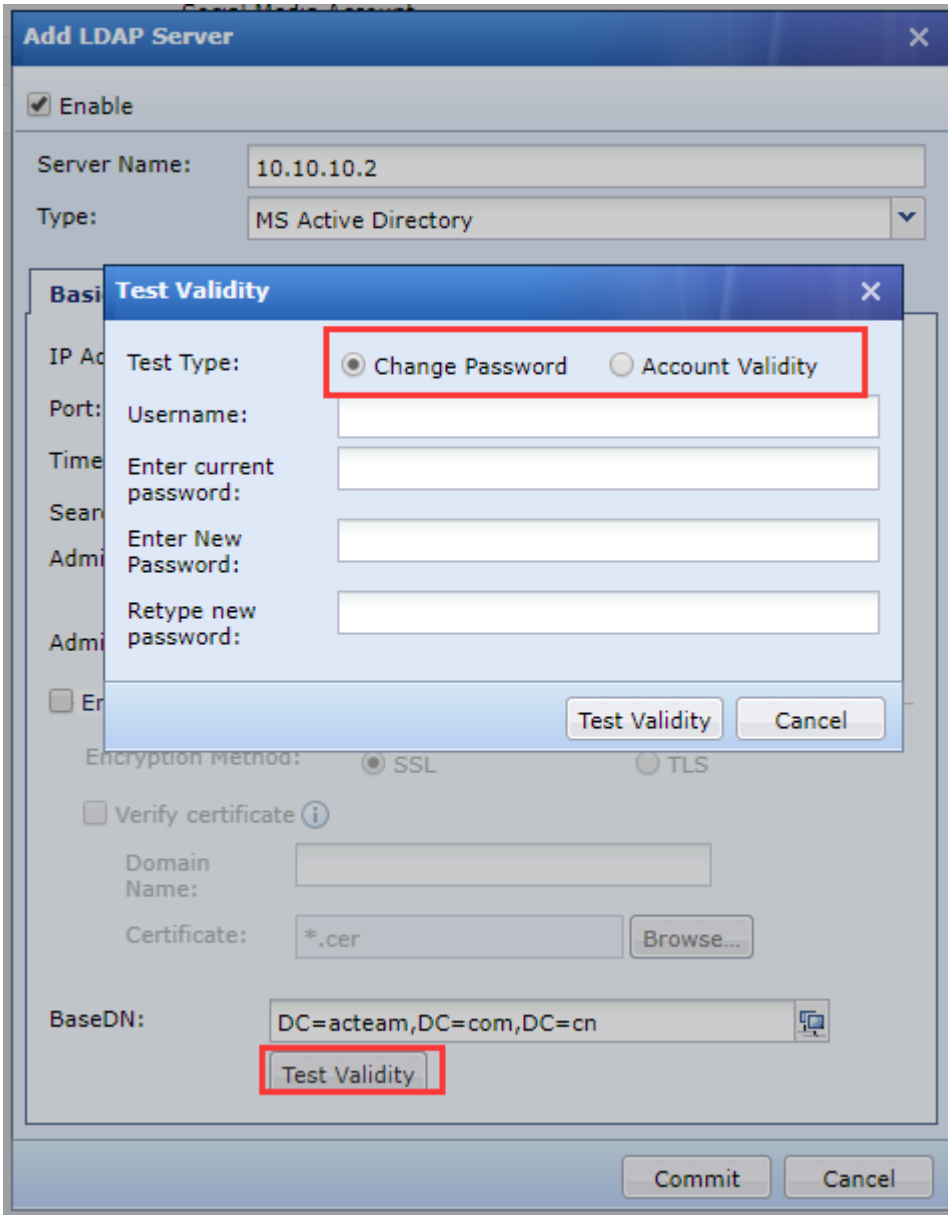
Verifikasi Certificate: Jika AD domain server dikonfigurasi dengan [LDAPS signing requirement option], Anda perlu konfigurasi item ini, isi domain name [AD domain server full computer name], dan import Certificate.



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



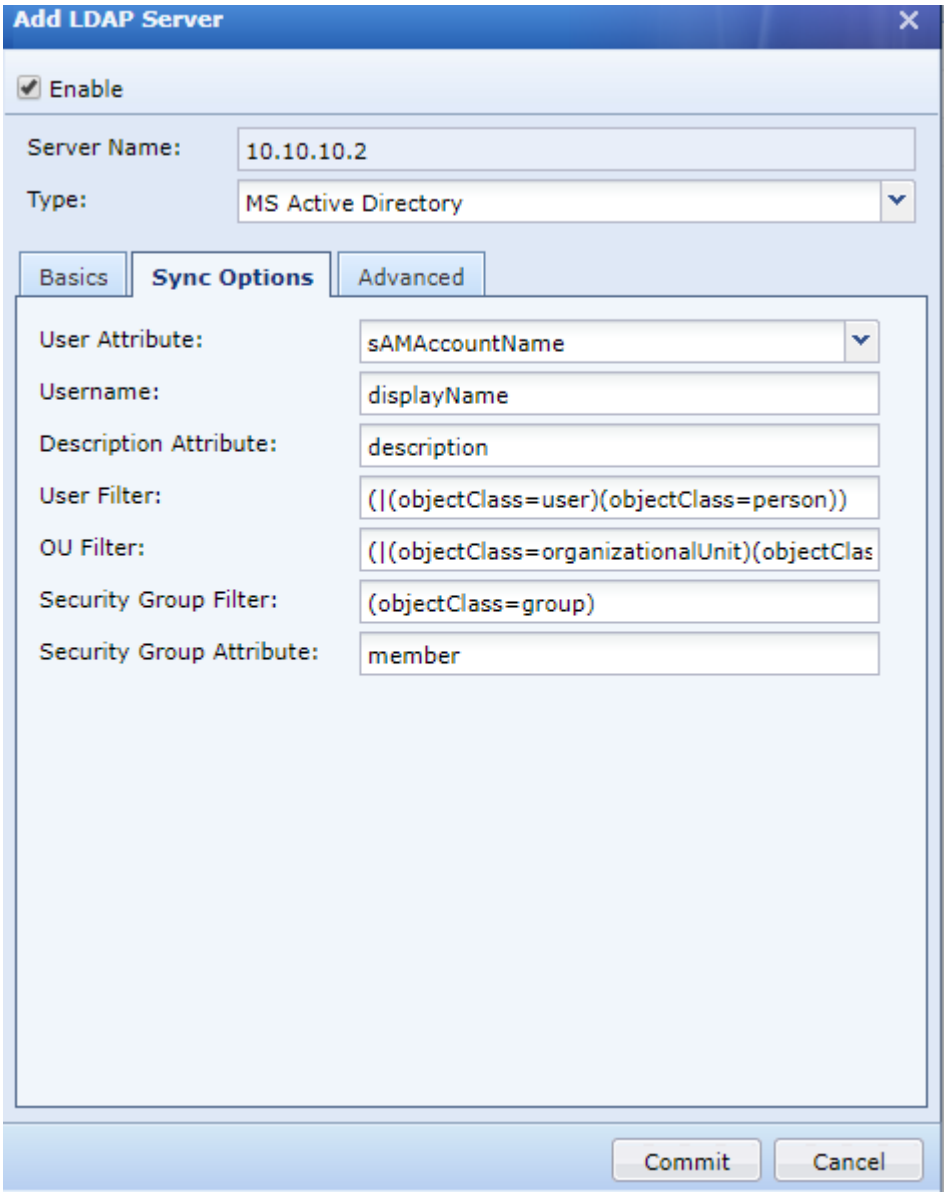
3. Test validity **[test validity].**



[Change Password]: Jika AD domain akun diperiksa untuk autentikasi pertama kali dan password dapat diubah, maka password dapat diubah langsung di sini.

[Account Validity]: Test apakah perangkat IAM dapat berkomunikasi langsung dengan AD domain dan memverifikasi bahwa akun tersebut valid.

4. Edit **[sync options]**(Jika tidak ada persyaratan khusus, tidak disarankan untuk edit dan memodifikasi, tetap pada default).



[User Attribute]: menentukan attribute field pada LDAP server yang secara unik mengidentifikasi pengguna. Misalnya, sAMAccountName attribute pada AD domain mengidentifikasi pengguna, dan di Novell LDAP, uid attribute mengidentifikasi pengguna.

[Username]: Menentukan attribute field pada LDAP server yang secara unik mengidentifikasi nama tampilan pengguna. Misalnya, displayName attribute pada AD domain mengindentifikasi nama tampilan pengguna.

[Description Attribute]: Menentukan attribute field pada LDAP server yang secara unik

mengidentifikasi deskripsi pengguna. Misalnya, description attribute pada AD domain mengidentifikasi deskripsi pengguna.

[User Filter]: Menentukan kondisi penyaringan pengguna dari LDAP server. Artinya, Anda dapat menentukan apakah sebuah node adalah pengguna. Misalnya, Anda dapat filter apakah node adalah pengguna dengan isi "(|(objectClass=user)(objectClass=person))" .

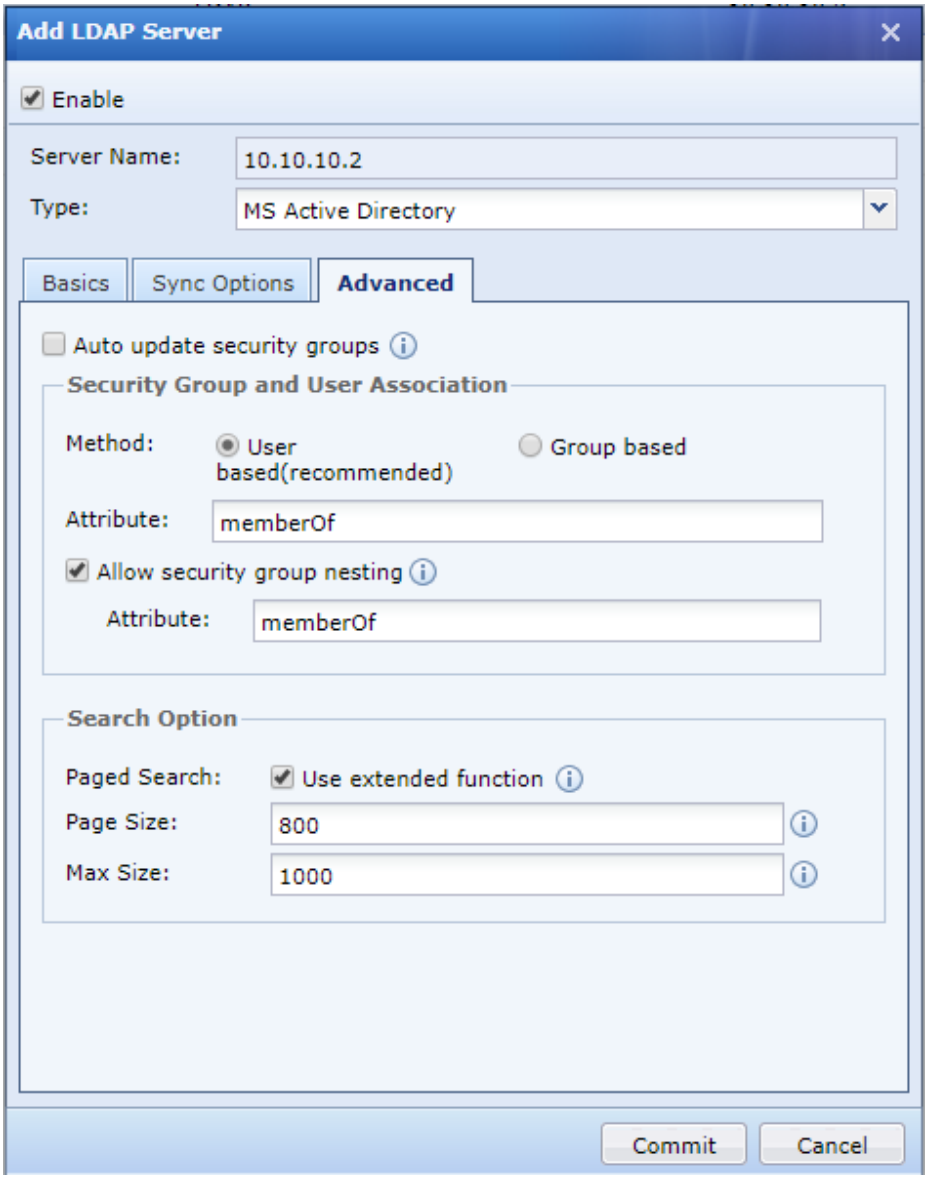
[OU Filter]: Menentukan kondisi organizational unti filter LDAP server, artinya, apakah node dapat menjadi organizational unit dengan menggunakan kondisi ini. Misalnya, the AD domain dapat disi oleh"(|(objectClass=organizationalUnit)(objectClass=organization)(objectClass=domain)(objectClass =domainDNS)(objectClass=container))" untuk filter apakah sebuah node adalah sebuah organizational unit.

[Security Group Filter]: Menentukan kondisi (security) group filter dari LDAP server (Catatan: untuk AD domain, di sini adalah security group, untuk non-AD domain, berikut adalah group), artinya, melalui kondisi ini, hal ini dapat ditentukan apakah node adalah group (secure), misalnya, AD domain dapat digunakan untuk filter apakah sebuah node adalah sebuah security group dengan di isi "(objectClass=group)".

[Security Group Attribute]: Menentukan attribute mana pada AD domain server yang mengidentifikasi daftar member dari security group. Attribute ini membutuhkan efek ketika LDAP server adalah AD domain. Jika tidak ada kasus khusus di field ini, Anda biasanya dapat mengisi member.

Ketika tipe server memilih "MS Active Directory", parameter di atas diatur. Umumnya, default parameter dapat digunakan. Jika server tipe lain dari LDAP, perlu disesuaikan menurut situasi sebenarnya, sehingga perangkat dapat membaca LDAP dengan benar.

5. Edit konfigurasi **[Advance]**.



[Auto update security groups]: Setelah memeriksa, LDAP server akan diminta secara real time untuk sinkronisasi isi dari yang diperlukan sinkronisasi ke lokal, tetapi akan meningkatkan tekanan pada LDAP server. Option ini hanya berlaku untuk AD domain.

[Security Group and User Association]: Konfigurasi default adalah direkomendasikan di sini.

[Method]: Anda dapat memilih "pengguna untuk menemukan (recommended)" atau "group to find users". Jika pengguna memiliki attribute pada LDAP server yang memiliki group yang seharusnya, Anda dapat memilih "User Group (Recommended)" karena metode ini akan memberikan kinerja yang lebih baik dan mengurangi tekanan kinerja pada LDAP server. Jika tidak ada informasi yang disimpan antara pengguna dan group pada LDAP server, hanya group yang menyimpan pengguna. Dalam hal ini, Anda perlu memeriksa group untuk menemukan pengguna.

[Attribute]: Jika "User based" mode dipilih, field ini membutuhkan untuk mengisi group di LDAP server atau pengguna menyimpan attribute dari group induk. Misalnya, memberOf attribute pada AD domain mengidentifikasi group induk dari sebuah node, jadi ketika mencari,

memberOf attribute digunakan untuk mencari group induk. Jika "Group based" dipilih, field ini harus diisi attribute dari group simpan subpengguna di LDAP server. Misalnya, member attribute pada AD domain mengidentifikasi sub-pengguna dari group, jadi ketika mencari, member attribute digunakan untuk mencari sub-pengguna dari group.

[Allow security group nesting]: check box menentukan apakah konfigurasi (security) group berlaku untuk pengguna di bawah group, atau apakah pengguna dan subgroup di bawah group bersifat rekursif. Jika Anda memilih field ini, pengguna dan sub-group dari group (secure) yang sesuai akan efektif secara rekursif. Jika tidak dicentang, ini berarti bahwa hanya pengguna bawahan dalam konfigurasi group (secure) yang valid, dan semua subgroup diabaikan.

[Nesting Attribute]: Nested properties hanya dapat diisi setelah "Allow security group nesting" diperiksa. Option ini mengindikasikan attribute yang dipakai oleh group yang perlu dicari untuk saat melihat ke atas secara rekursif. Jika mode "User based"dipilih , field ini hanya perlu konsisten dengan "Associated Properties". Jika "Group based" dipilih, field perlu mengisi attribute dari group simpan subgroup di LDAP server. Misalnya, member attribute pada AD domain mengidentifikasi semua subgroup dari suatu group, jadi saat mencari, member attribute digunakan untuk mencari semua subgroup dari suatu group.

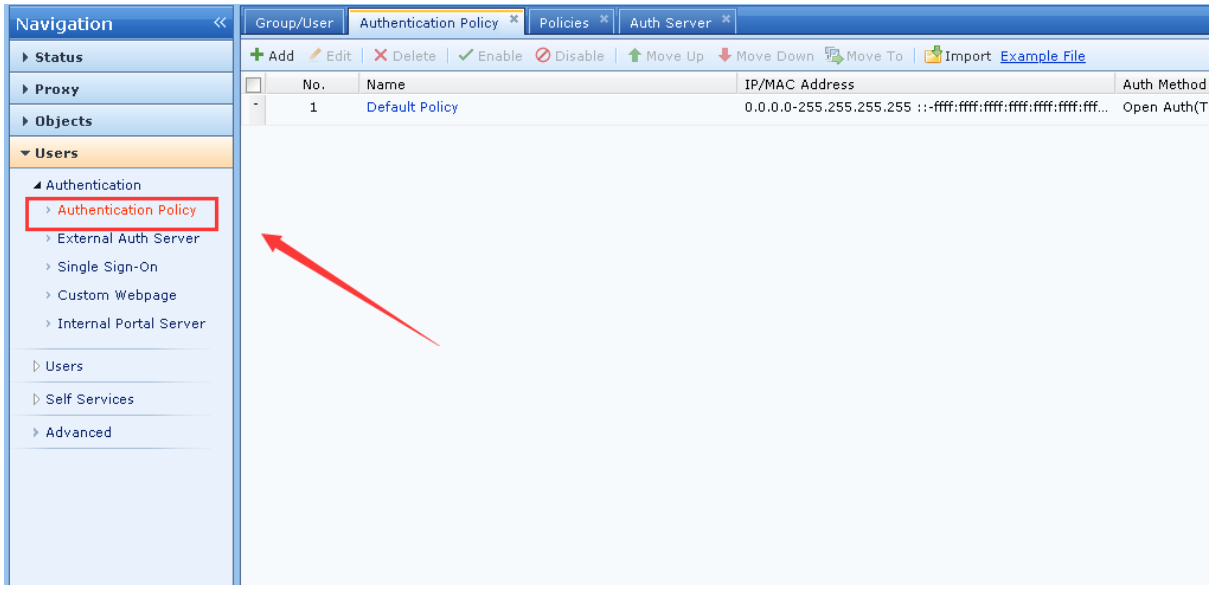
[Page search]: Untuk mencari LDAP server menggunakan extension API, direkomendasikan untuk mempertahankan konfigurasi default.

[Page size]: Ukuran dikembalikan ketika LDAP page, 0 berarti tidak ada batas, direkomendasikan untuk tetap menggunakan konfigurasi default.

[Max size]: Batas ukuran option ketika menyinkronkan LDAP, direkomendasikan untuk tetap menggunakan konfigurasi default.

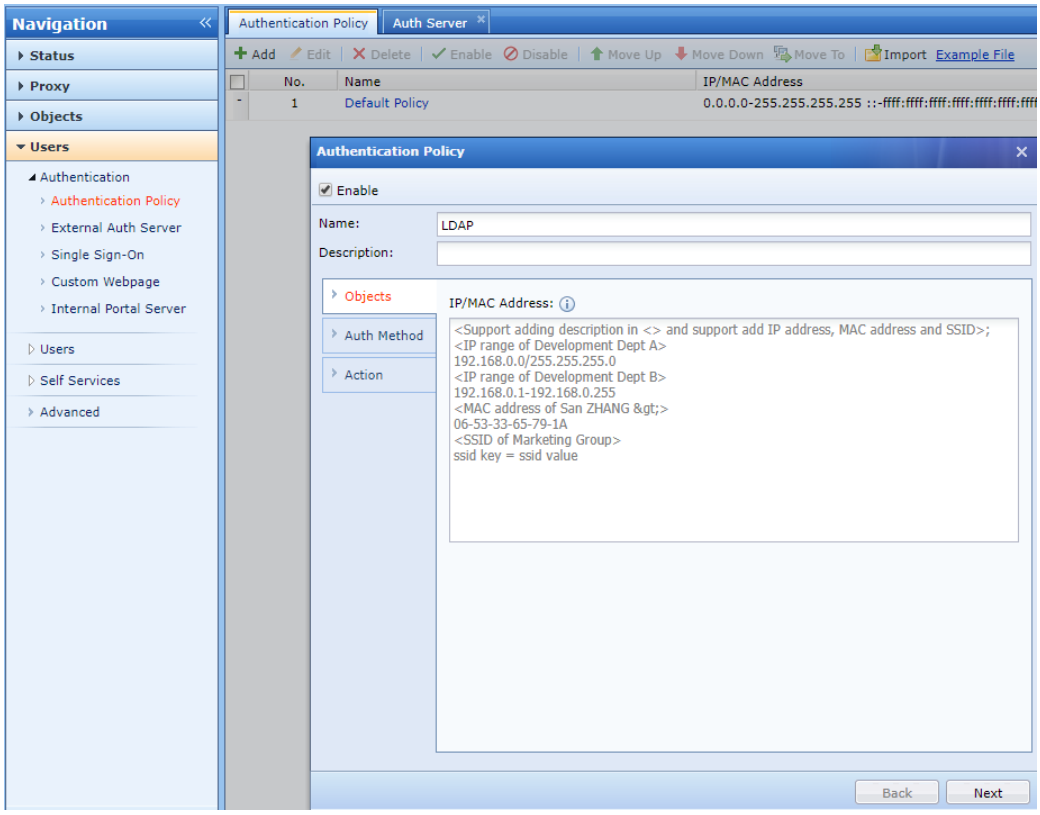
2.2 User Authentication Configuration

1. Edit **Users > Authentication > Authentication policy.**

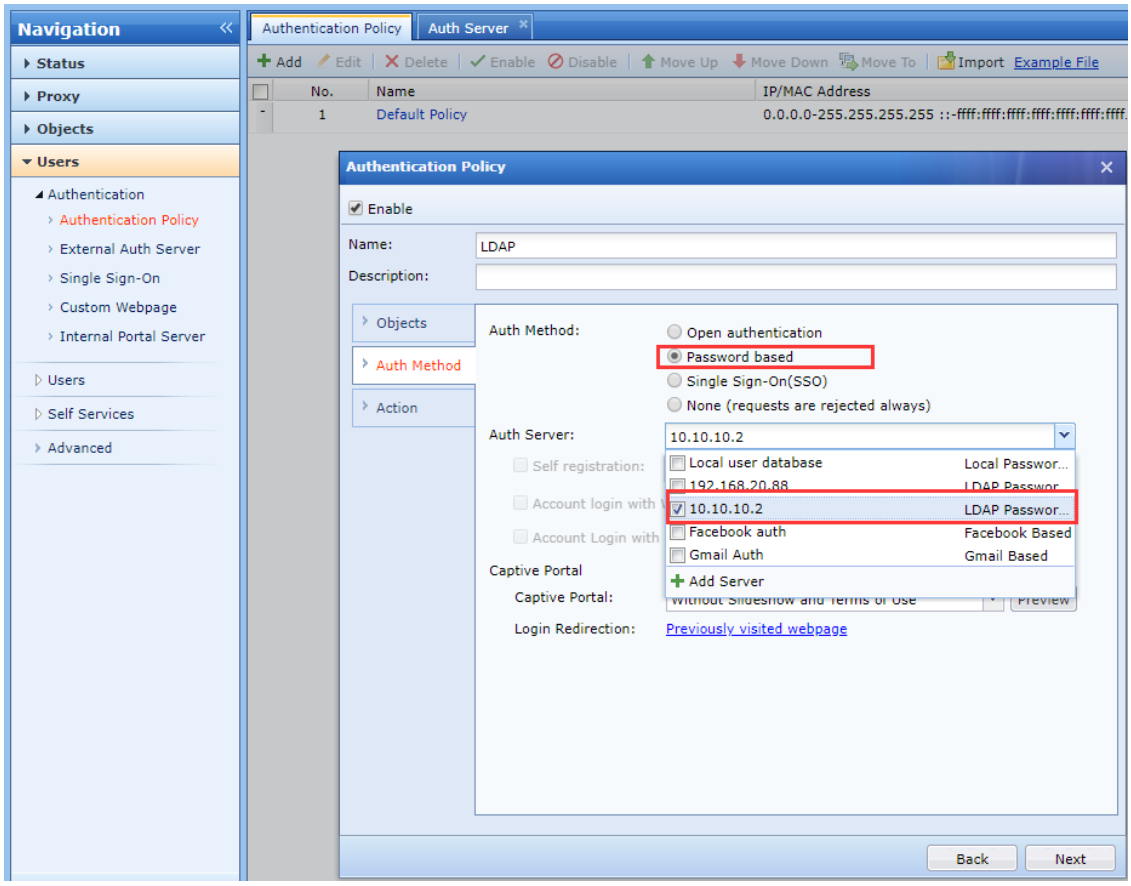


2. **Add > Authentication Policy** – Direkomendasikan untuk menguji proses di awal dari

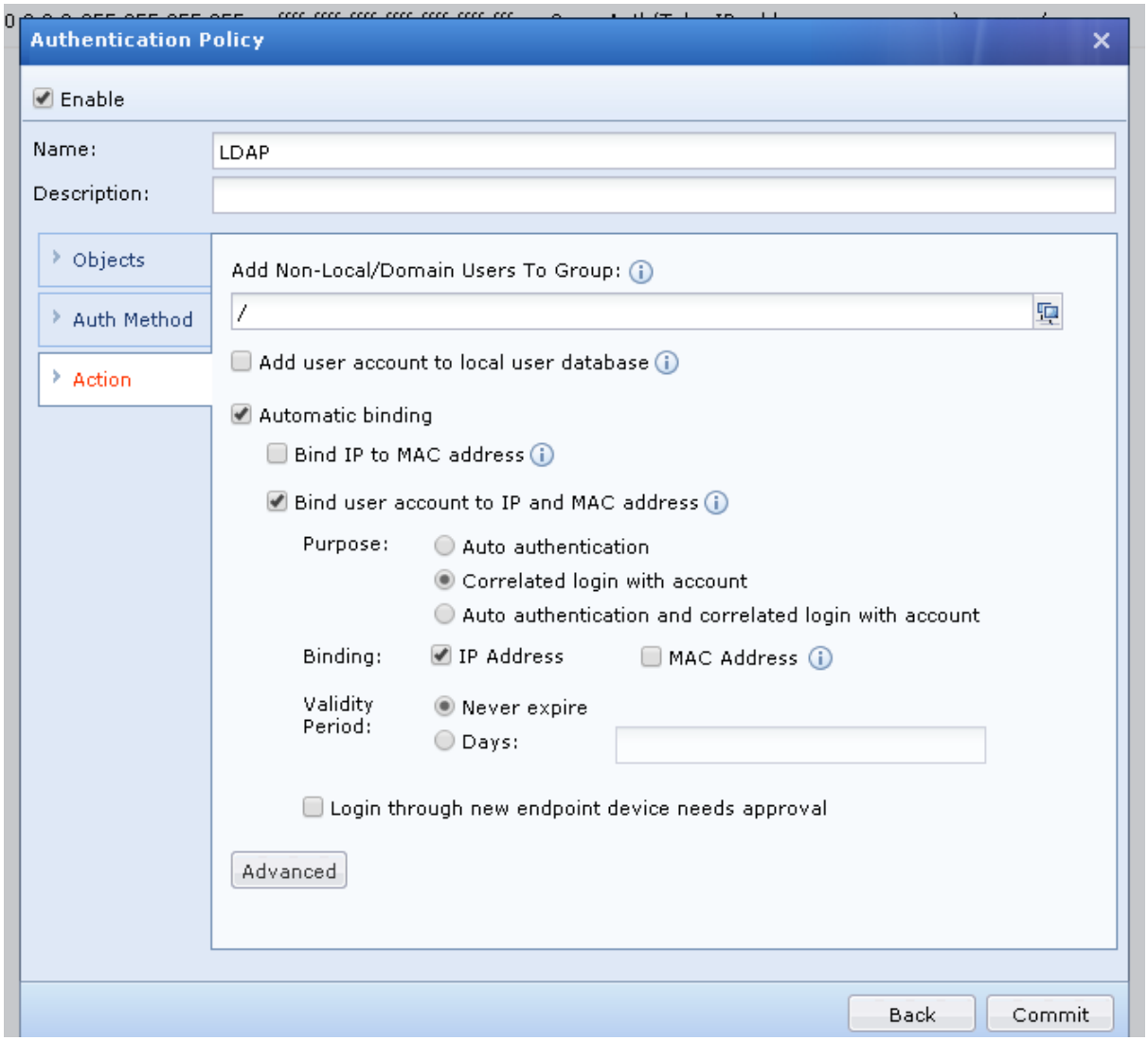
tes untuk single address. Setelah tes berhasil, secara bertahap memperluas jangkauan tes.



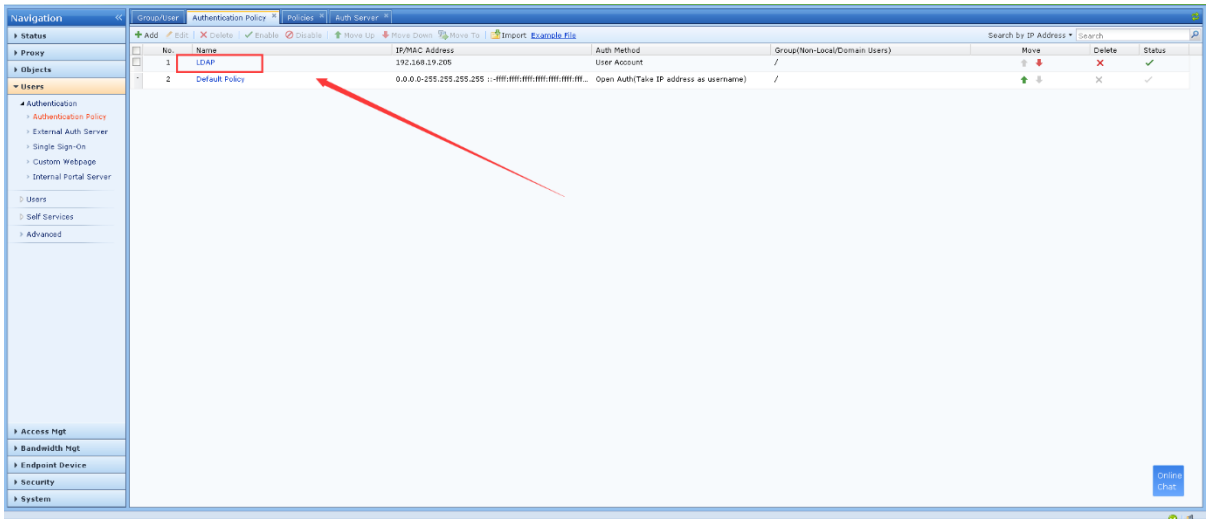
3. **Authentication method**: Pilih authentication method: Password based. Auth server: Pilih - LDAP domain server dibuat di external auth server.



4. Tindakan persyaratan konfigurasi setelah proses autentikasi.

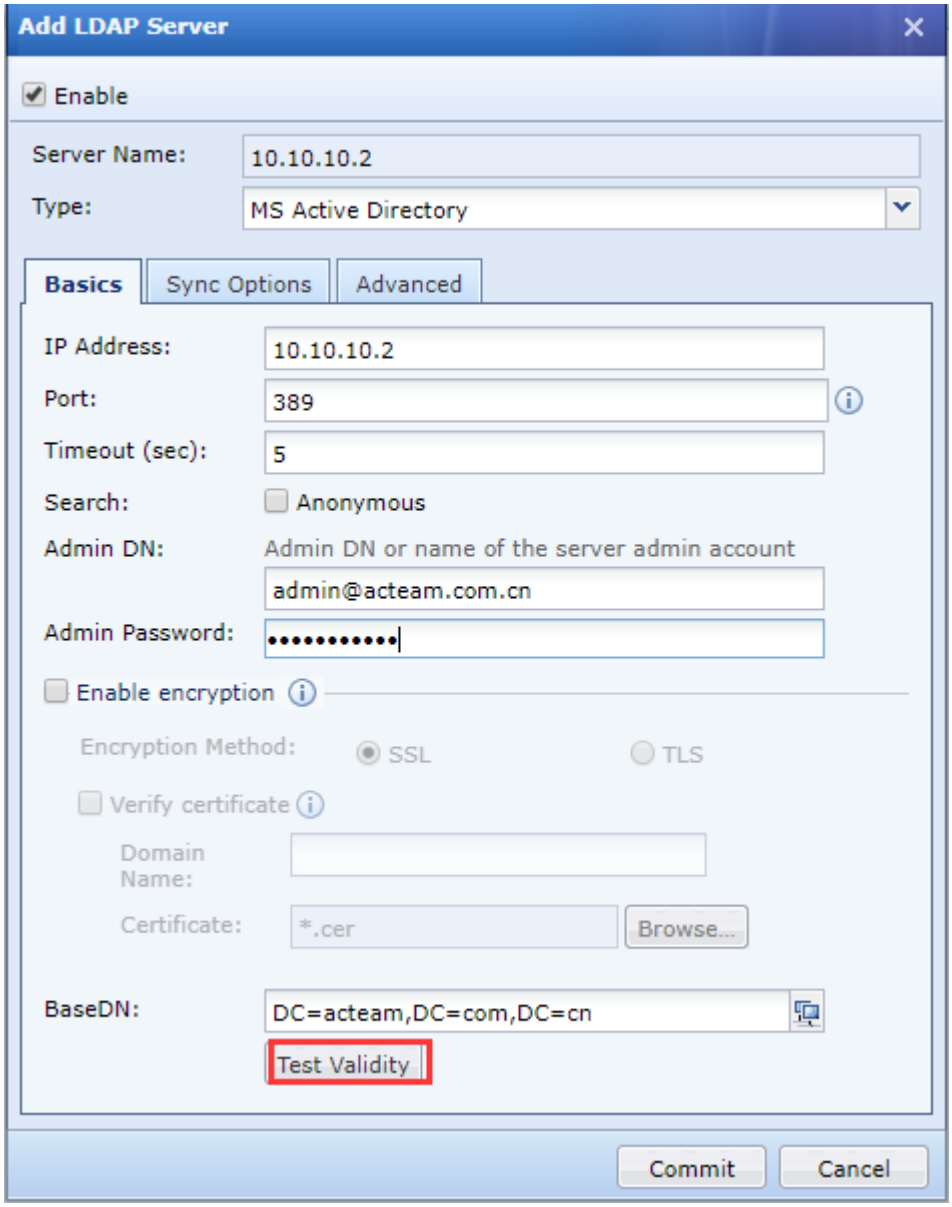


5. Anda dapat melihat new policy di antarmuka autentikasi policy.

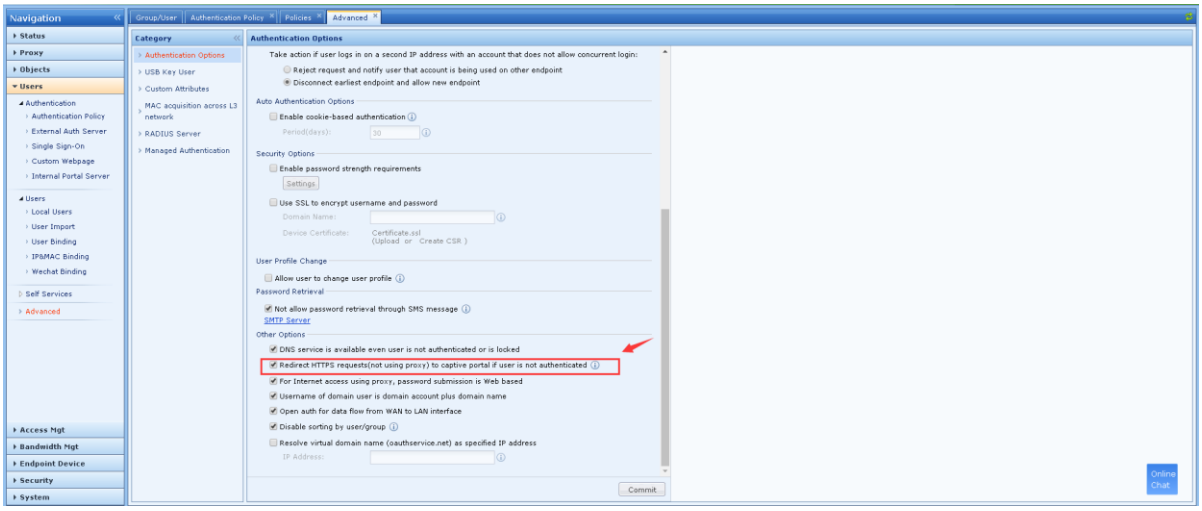


Bab 3 Tindakan Pencegahan

1. Ketika konfigurasi external authentication server administrator akun dan password, direkomendasikan untuk klik - [test validity] untuk memastikan bahwa itu tersedia. Seperti yang ditunjukkan gambar:



2. Klien membuka web page untuk membuka autentikasi page. Jika ini adalah domain URL link untuk membuka link, Anda perlu dapat menemukan domain name dan membuka URL dari http. Jika Anda perlu membuka URL dari https, Anda perlu pergi ke autentikasi page. Anda perlu memilih autentikasi option. Options pada gambar di bawah ini:



3. Jika signing requirement diaktifkan, IAM hanya dapat terhubung ke AD domain. Secara khusus, Windows 2000/2003/2008 tidak mendukung TLS enkripsi, dan hanya SSL enkripsi dapat digunakan; Windows Server 2008 R2 dan di atas mendukung keduanya TLS dan SSL enkripsi.

Bab 4 Lampiran A: Panduan Konfigurasi LDAP

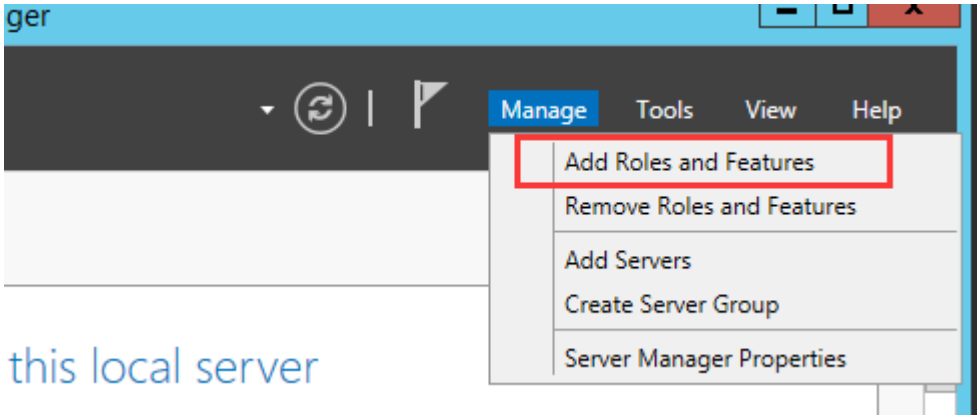
4.1 Latar Belakang

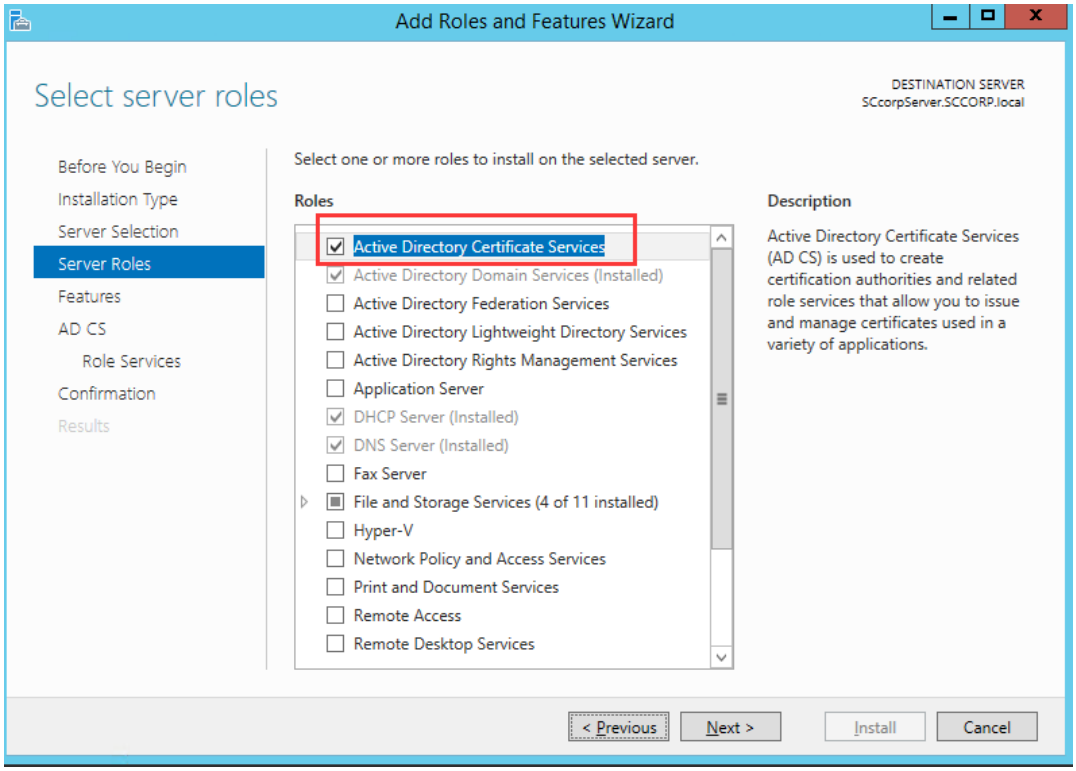
Pada bulan 2019, Microsoft mengumumkan di buletin security [ADV190023 | Microsoft Guidance for Enabling LDAP Channel Binding and LDAP Signing] bahwa LDAP channel binding dan LDAP signing akan diaktifkan di Active Directory server melalui metode security update(KB patch) pada pertengahan Januari 2020. Security of Active Directory domain controllers dapat ditingkatkan secara signifikan dengan konfigurasi server untuk menolak Simple Authentication dan 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.

4.2 Konfigurasi Instalasi Certificate Server

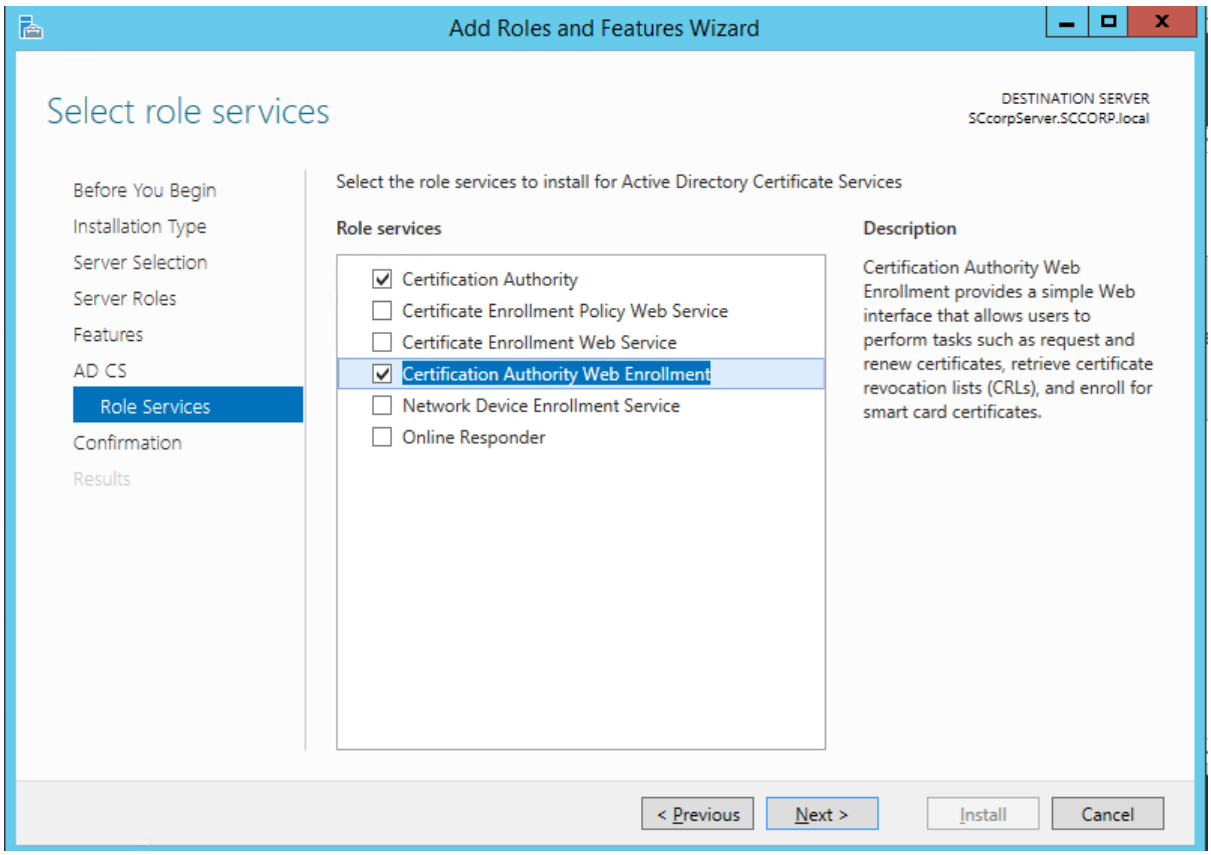
Setelah instal certificate service, server root certificate dapat dieksport untuk verifikasi certificate klien untuk meningkatkan security. Untuk bagaimana menginstal certificate service pada Active Directory server, mengacu pada tutorial berikut:

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

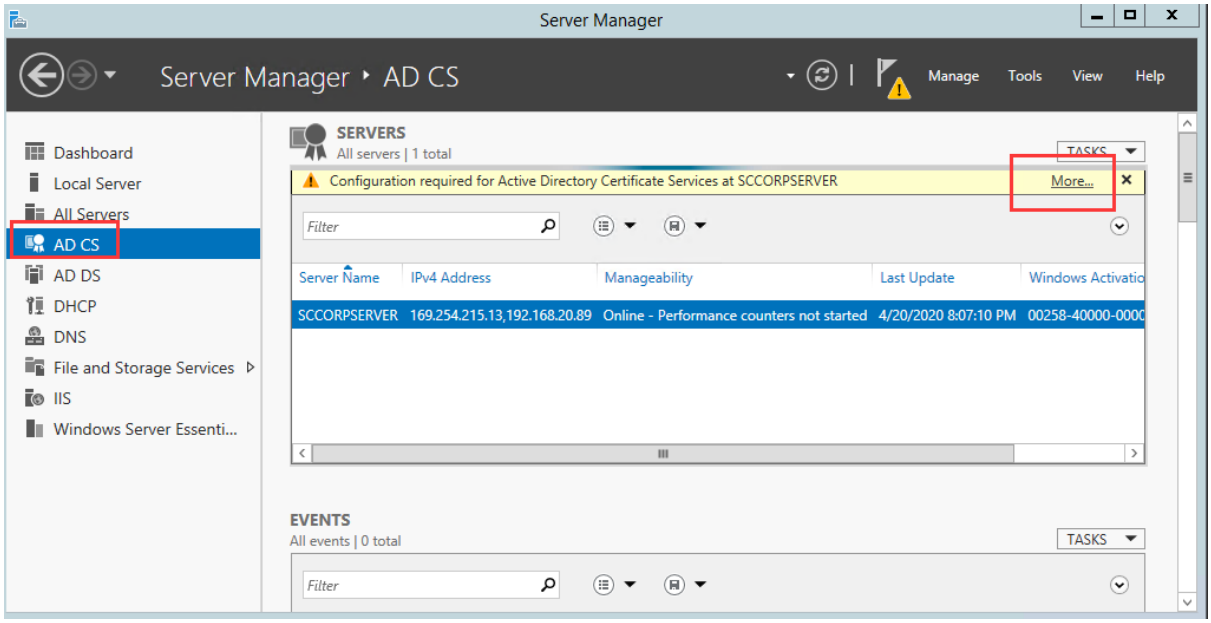

ger
Manage
Tools
View
Help
Add Roles and Features
Remove Roles and Features
Add Servers
Create Server Group
Server Manager Properties
this local server

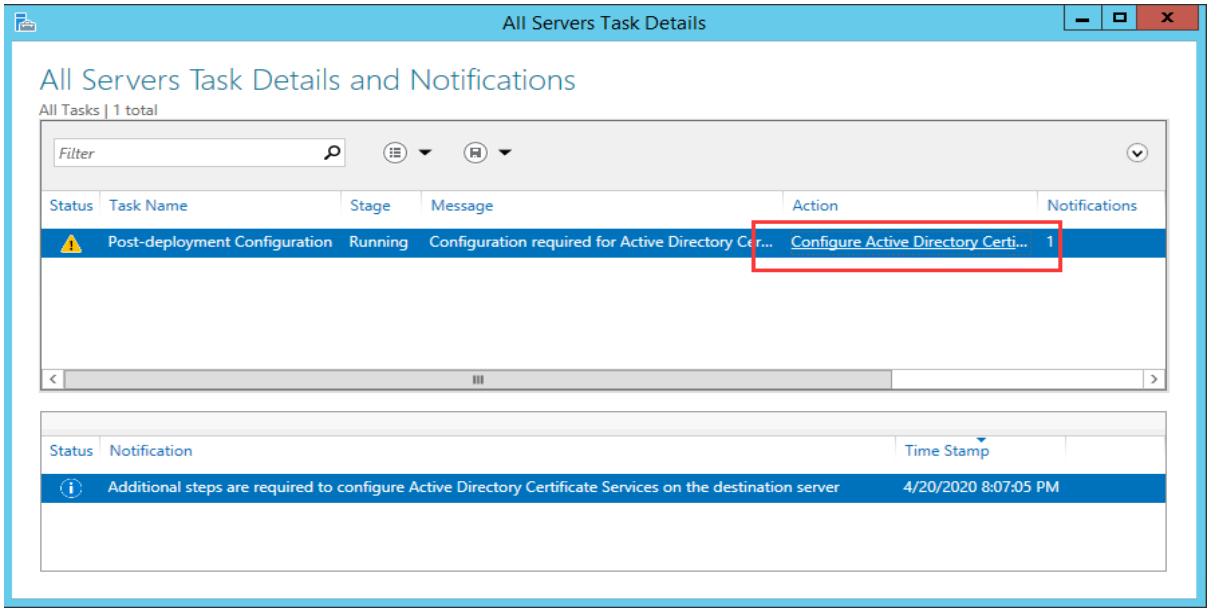

Add Roles and Features Wizard
Select server roles
DESTINATION SERVER
SCcorpServer.SCCORP.local
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD CS
Role Services
Confirmation
Results
Select one or more roles to install on the selected server.
Roles
Active Directory Certificate Services
Active Directory Domain Services (Installed)
Active Directory Federation Services
Active Directory Lightweight Directory Services
Active Directory Rights Management Services
Application Server
DHCP Server (Installed)
DNS Server (Installed)
Fax Server
File and Storage Services (4 of 11 installed)
Hyper-V
Network Policy and Access Services
Print and Document Services
Remote Access
Remote Desktop Services
Description
Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.
< Previous
Next >
Install
Cancel

Pilih Certificate Authority dan Certificate Authority Web Enrollment:

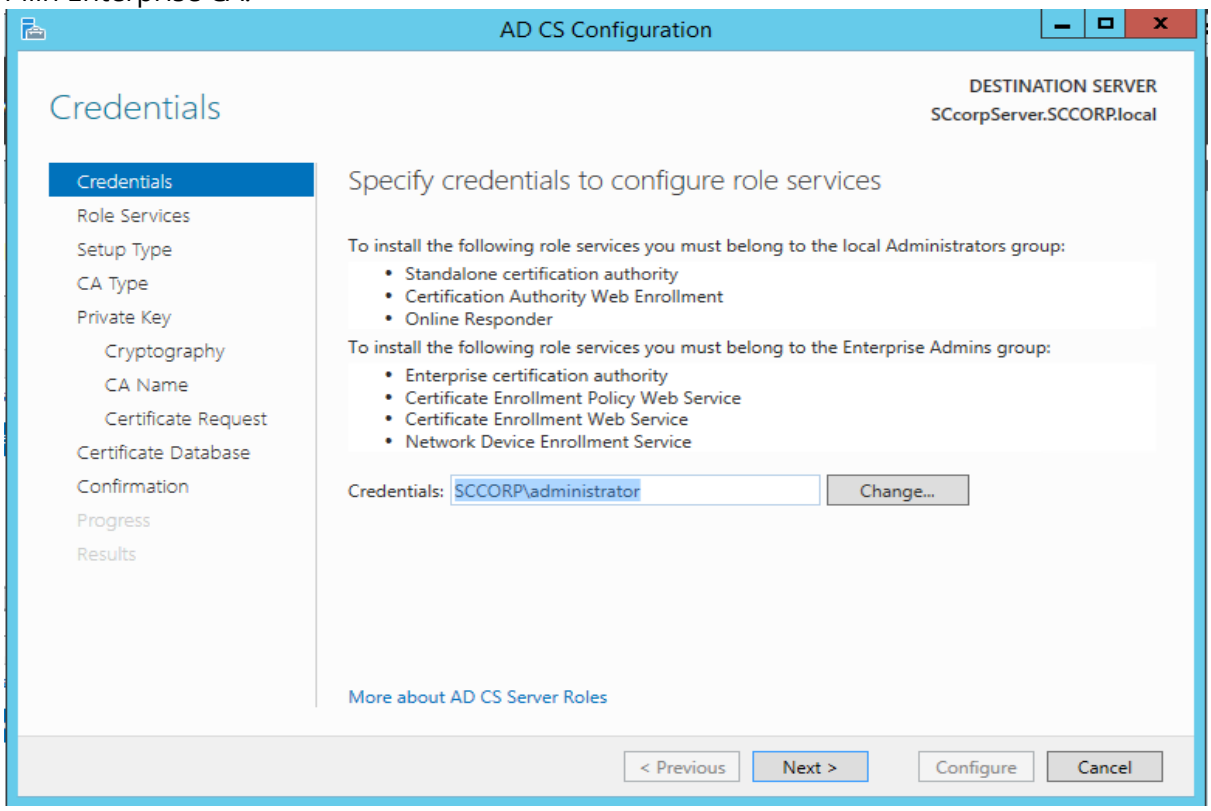


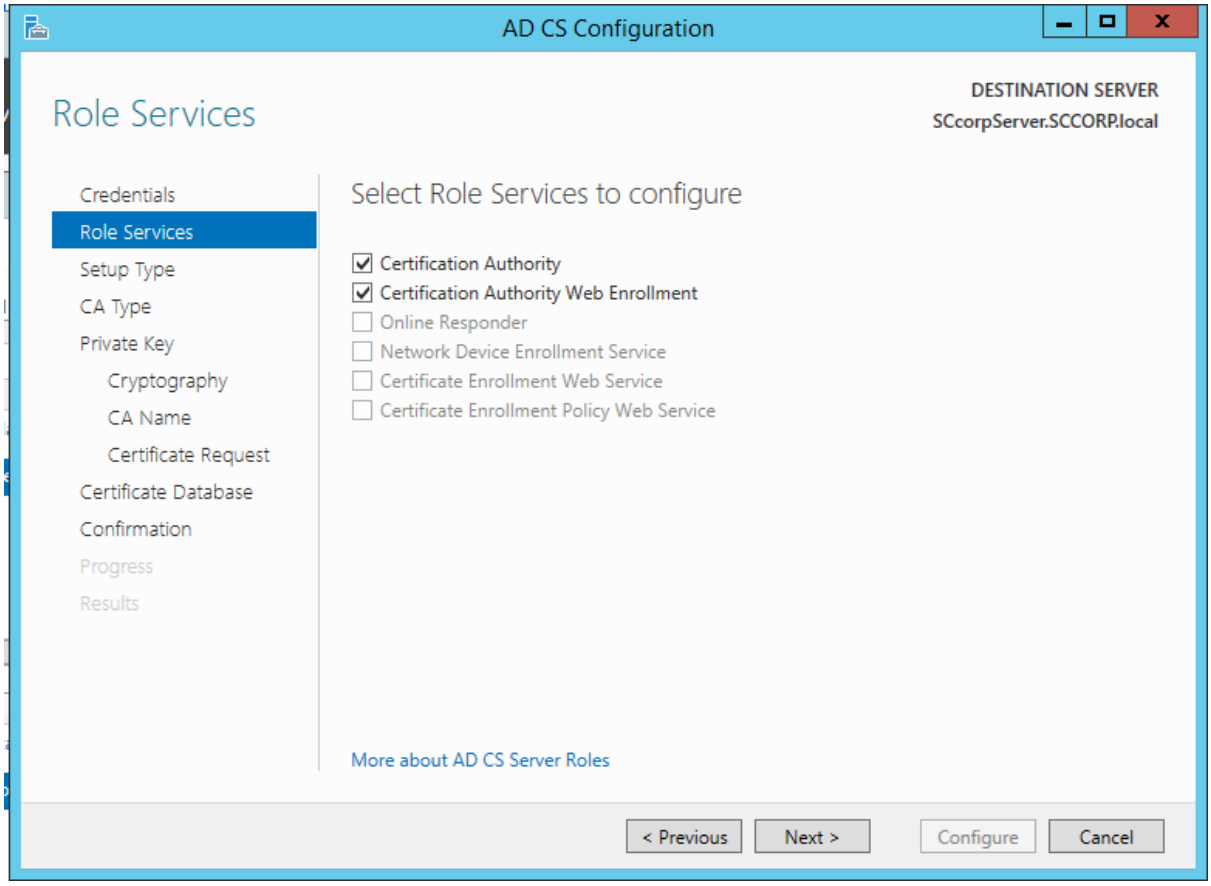
Pergi ke AD CS, pilih more dan klik Konfigurasi Active Directory Certification:

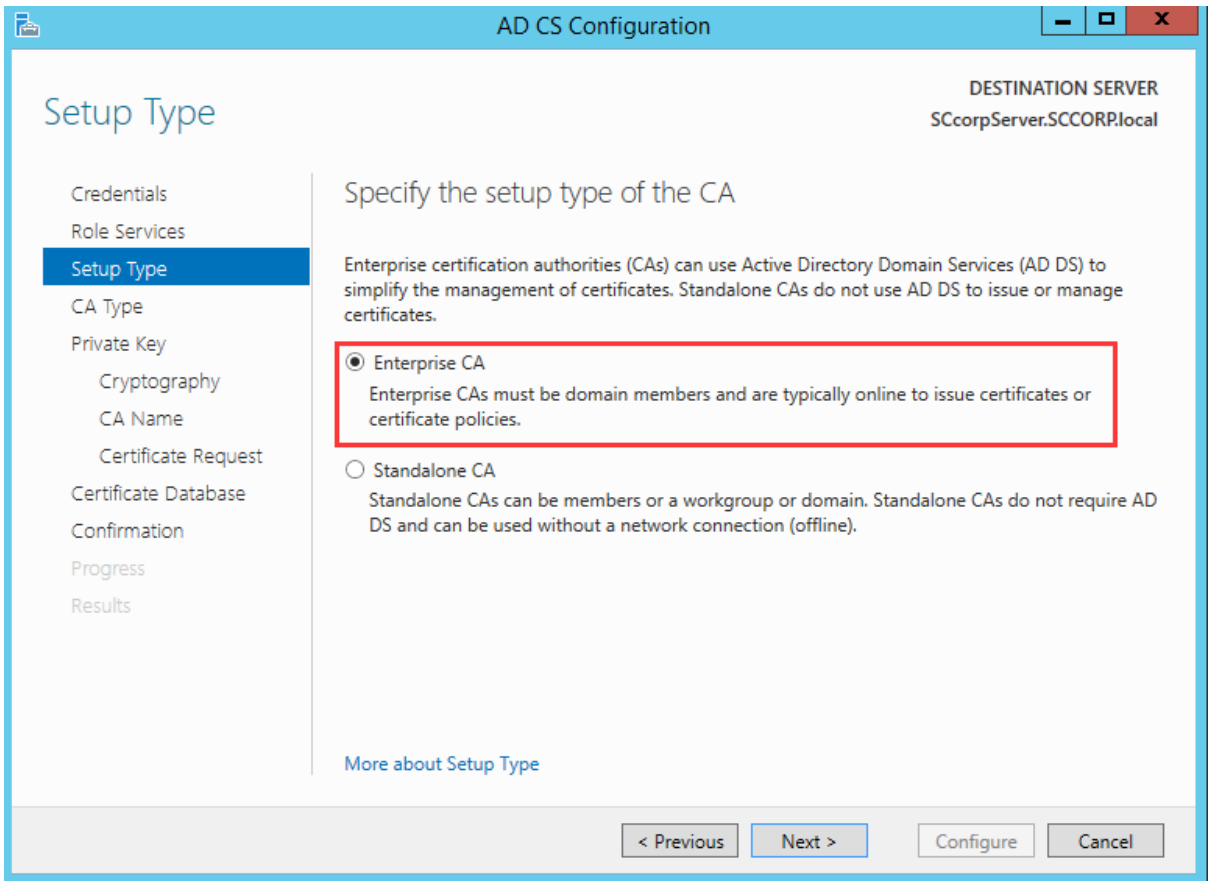




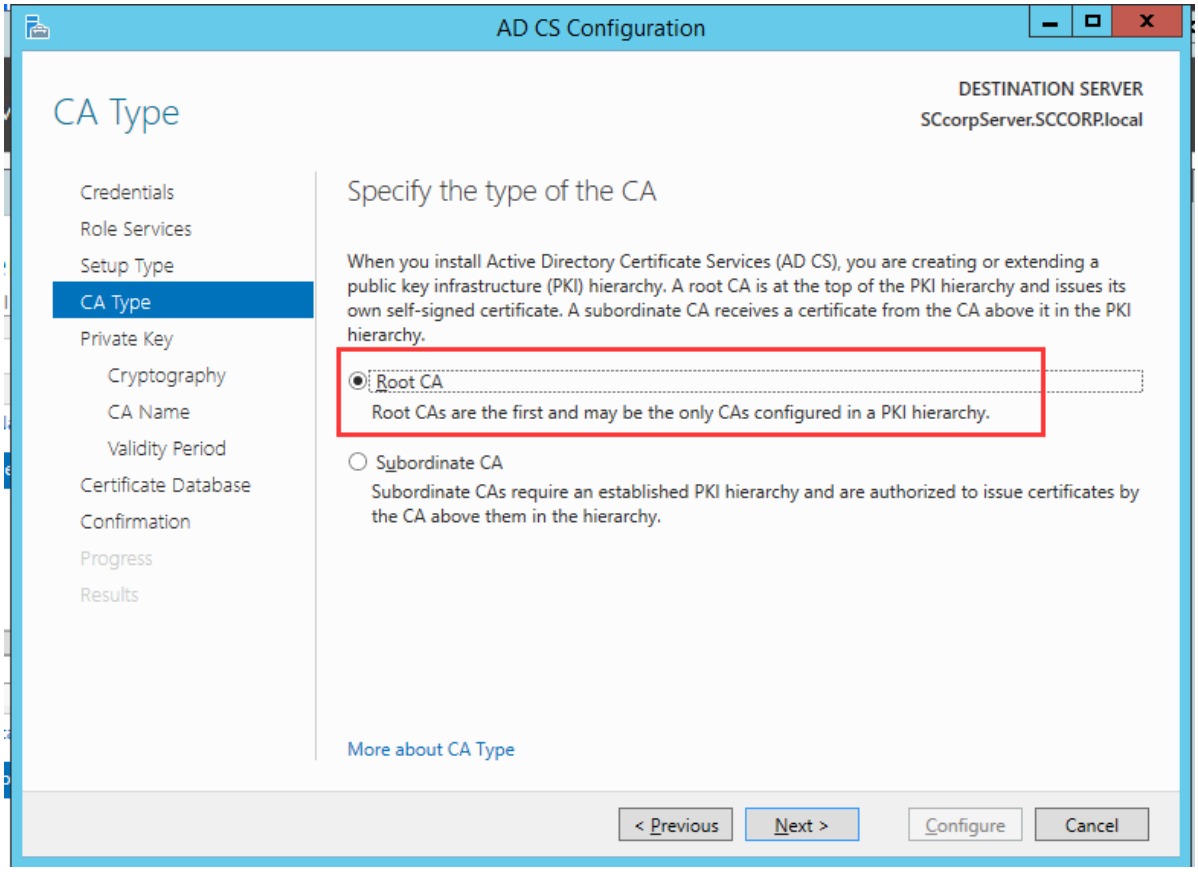
Pilih Enterprise CA:

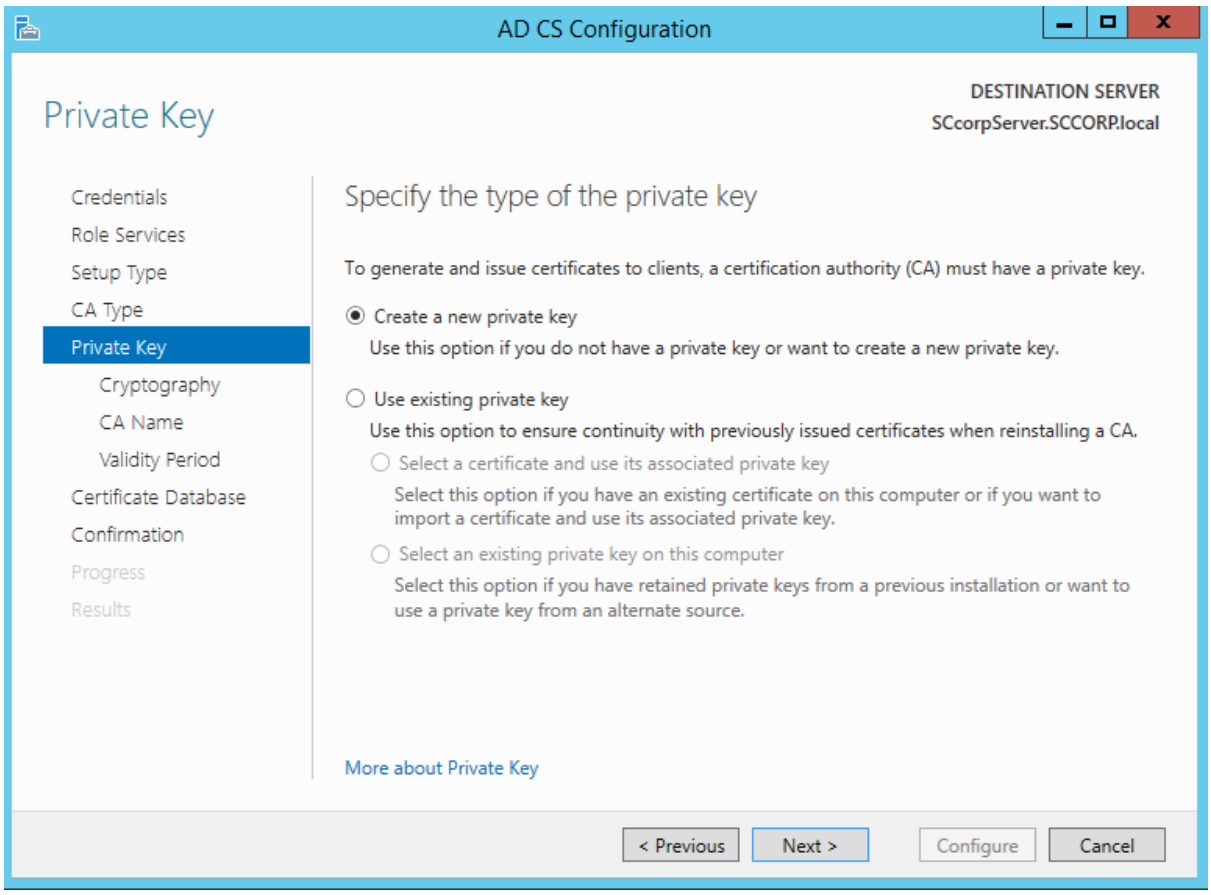




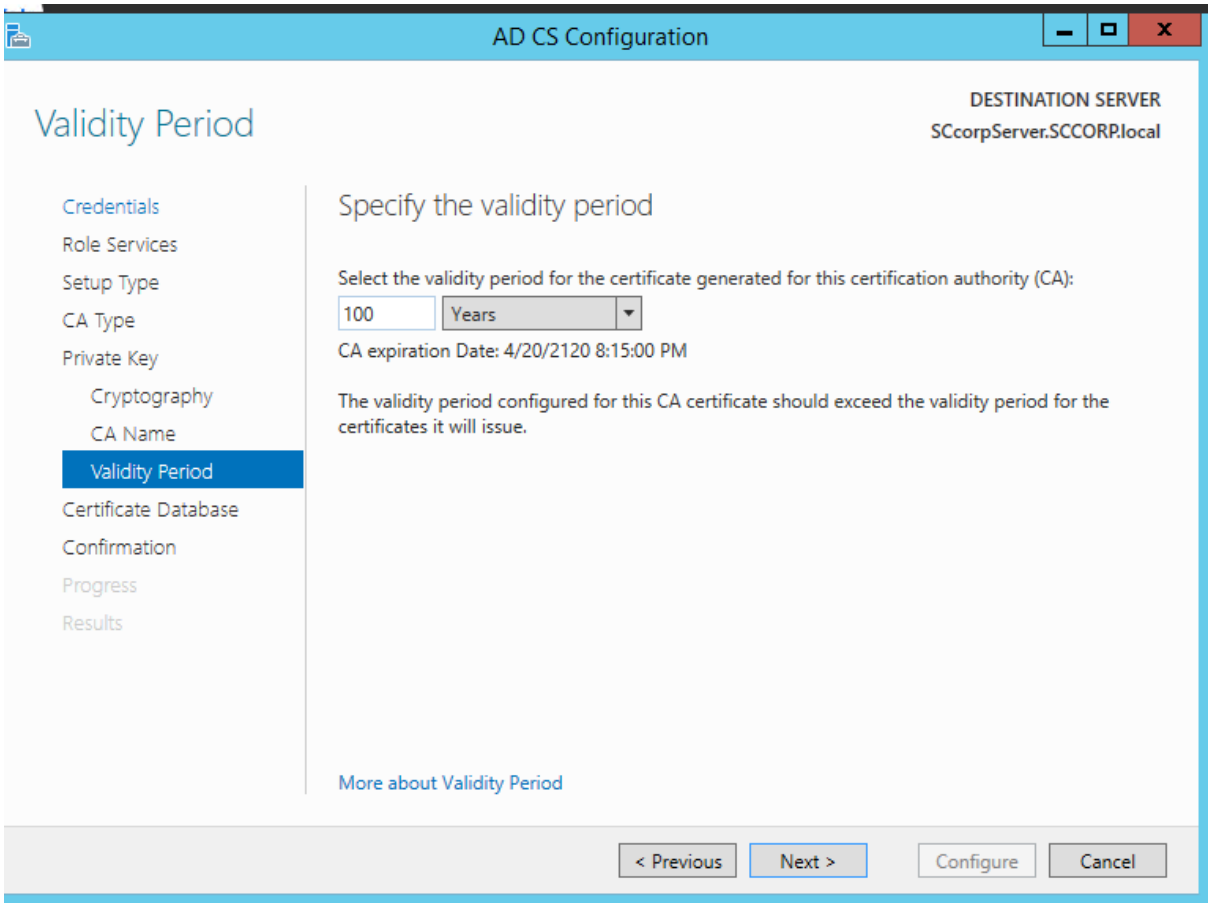


Pilih Root CA dan create New Private Key:

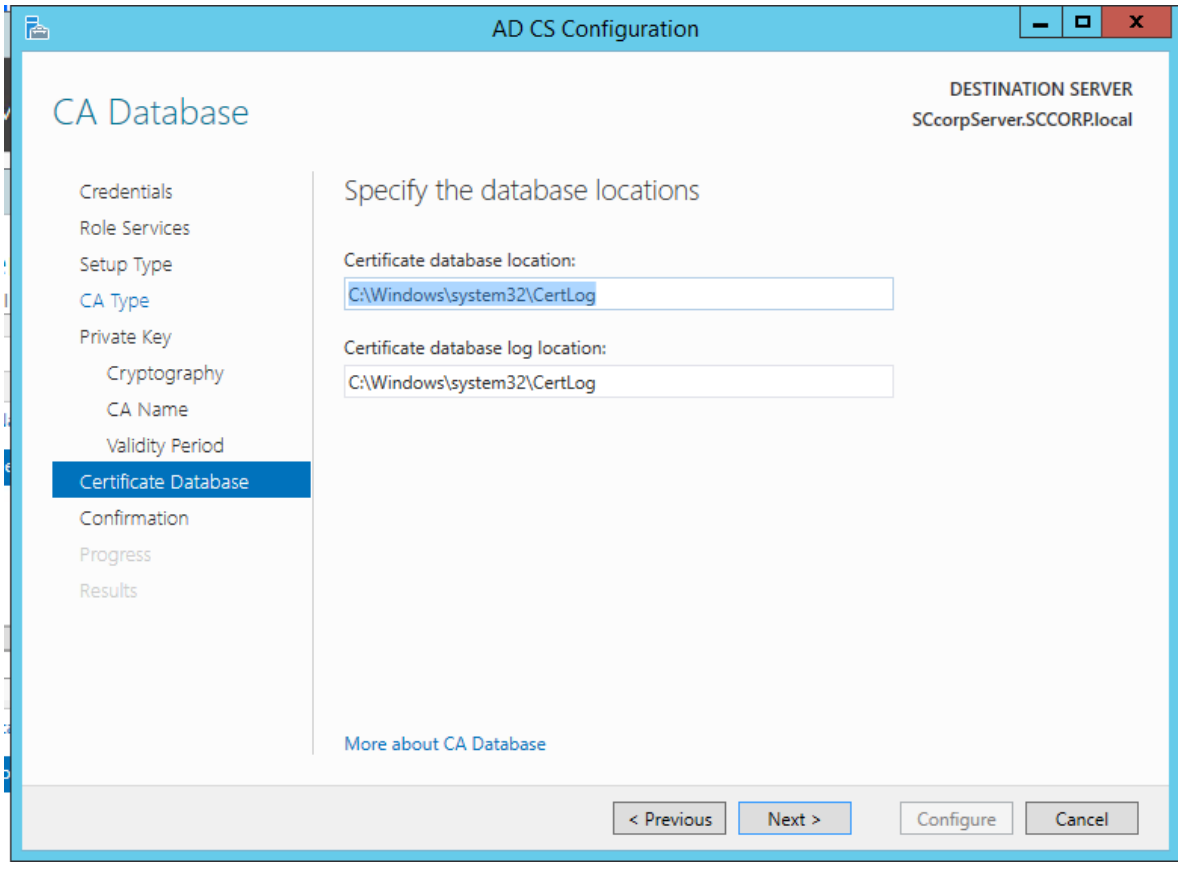

AD CS Configuration
CA Type
DESTINATION SERVER
SCcorpServer.SCCORP.local
Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results
Specify the type of the CA
When you install Active Directory Certificate Services (AD CS), you are creating or extending a public key infrastructure (PKI) hierarchy. A root CA is at the top of the PKI hierarchy and issues its own self-signed certificate. A subordinate CA receives a certificate from the CA above it in the PKI hierarchy.
Root CA
Root CAs are the first and may be the only CAs configured in a PKI hierarchy.
Subordinate CA
Subordinate CAs require an established PKI hierarchy and are authorized to issue certificates by the CA above them in the hierarchy.
More about CA Type
< Previous
Next >
Configure
Cancel


AD CS Configuration
Private Key
DESTINATION SERVER
SCcorpServer.SCCORP.local
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

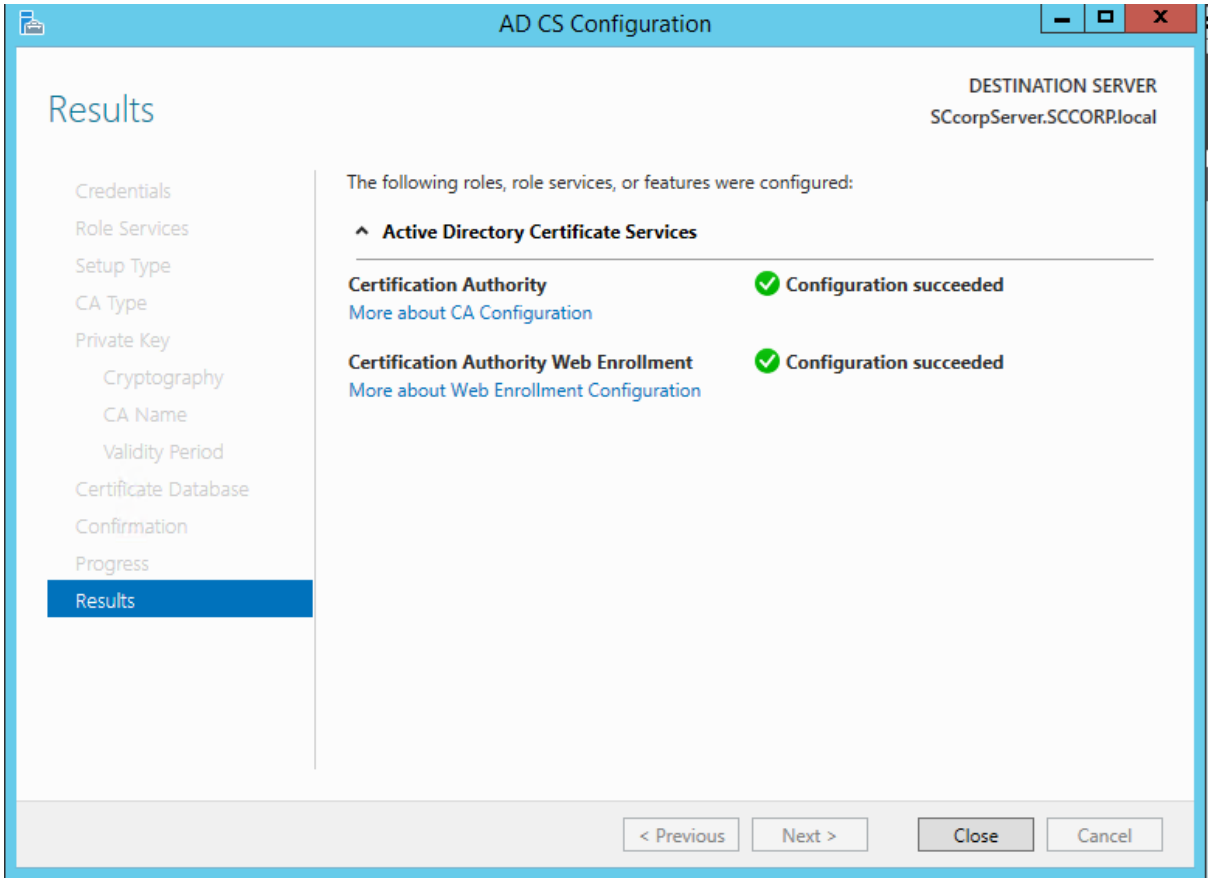
Mengatur validity period:



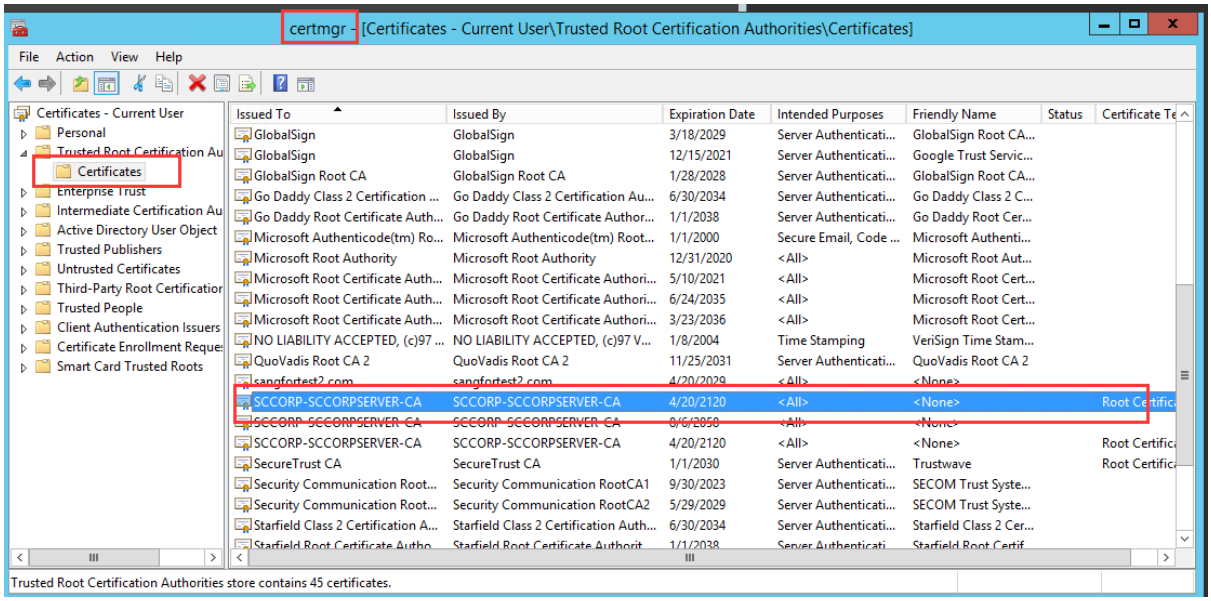
Specify the database location:



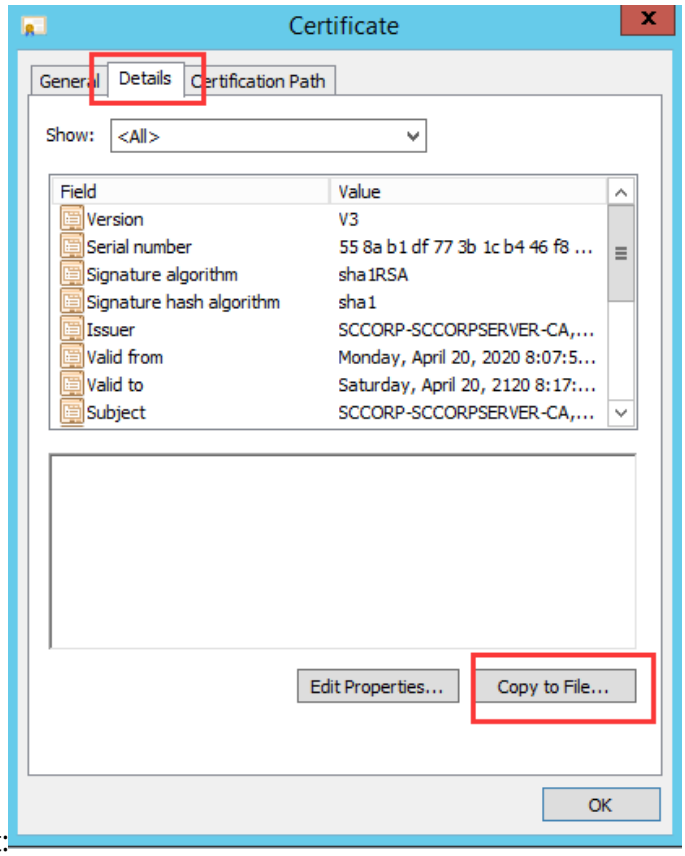
Installation complete:

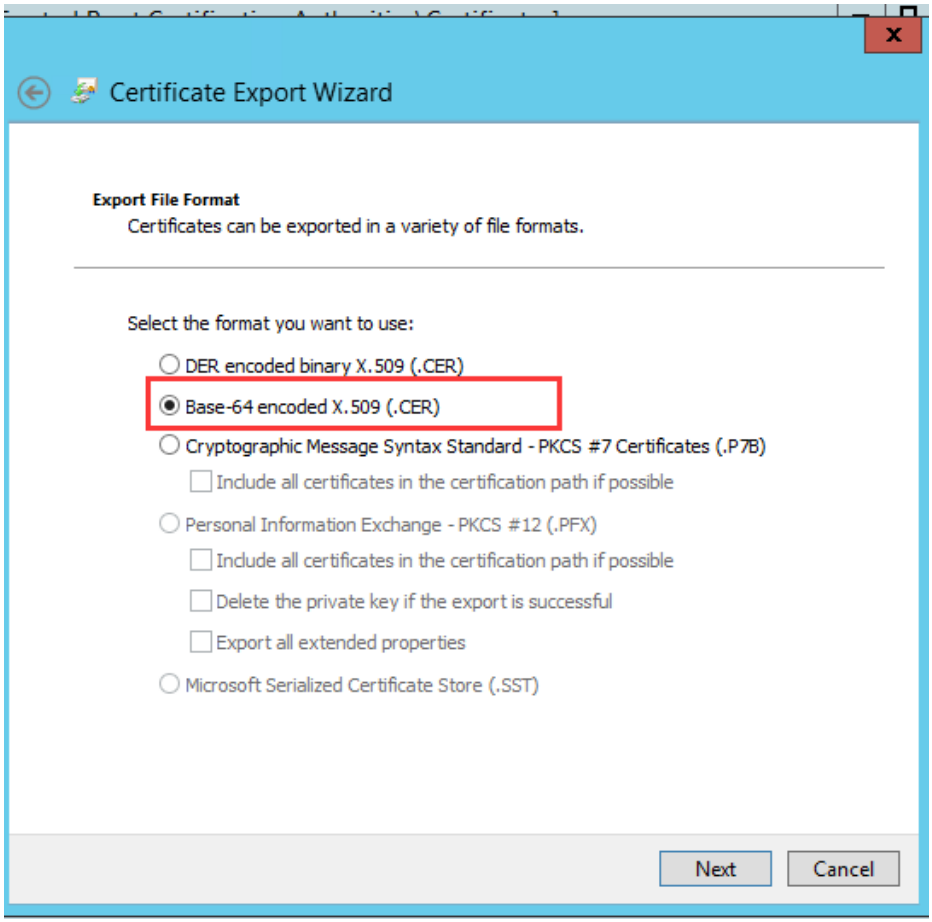


Pergi ke certmgr.msc:



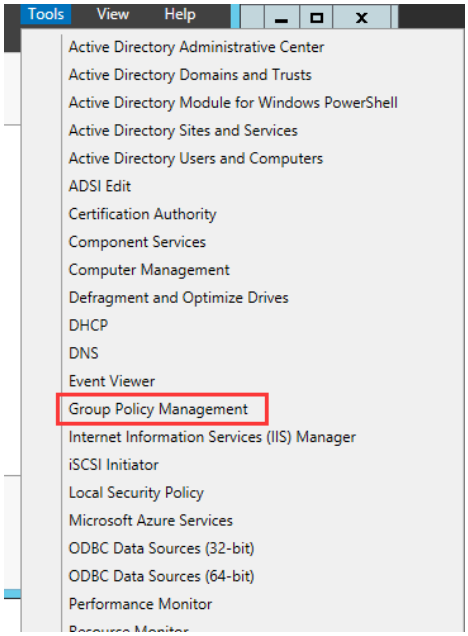
Buka cert dan klik pada Details -> Copy ke File dan export sebagai Base-64 dengan .cer format:



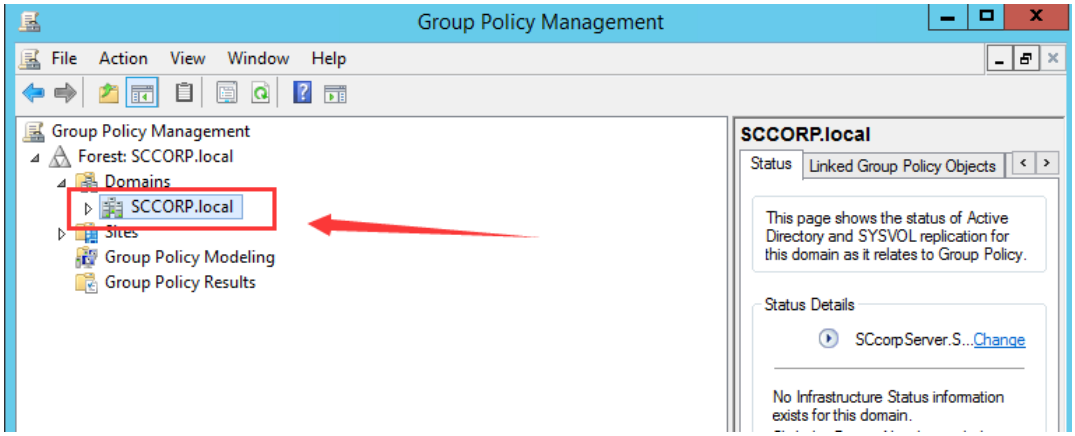


4.3 Konfigurasi LDAPS Server Signing

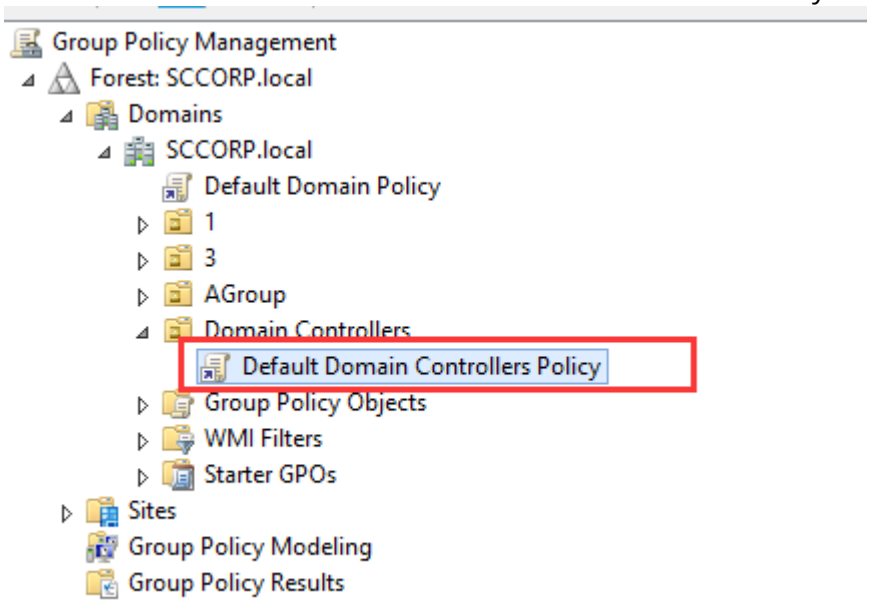
Pergi ke Server Manager ->Tools -> Klik Group Policy Management:



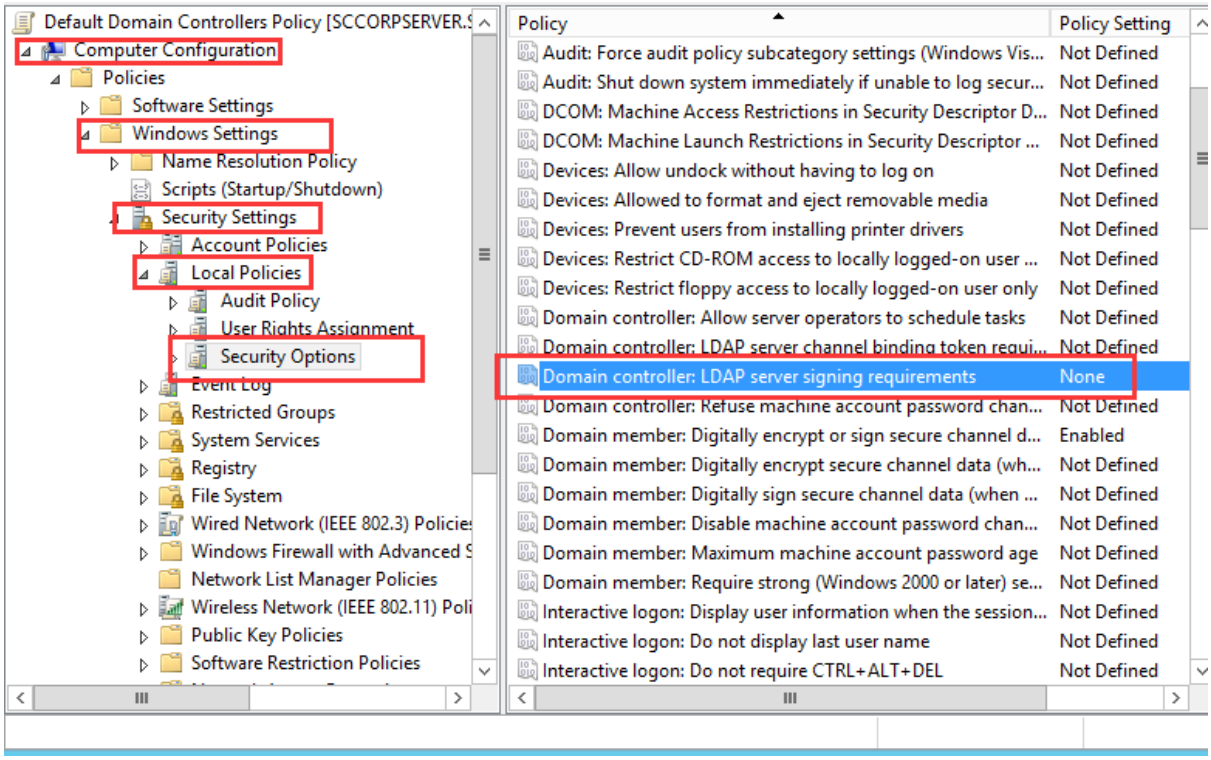
Pilih yang benar Domain name dan perpanjang.



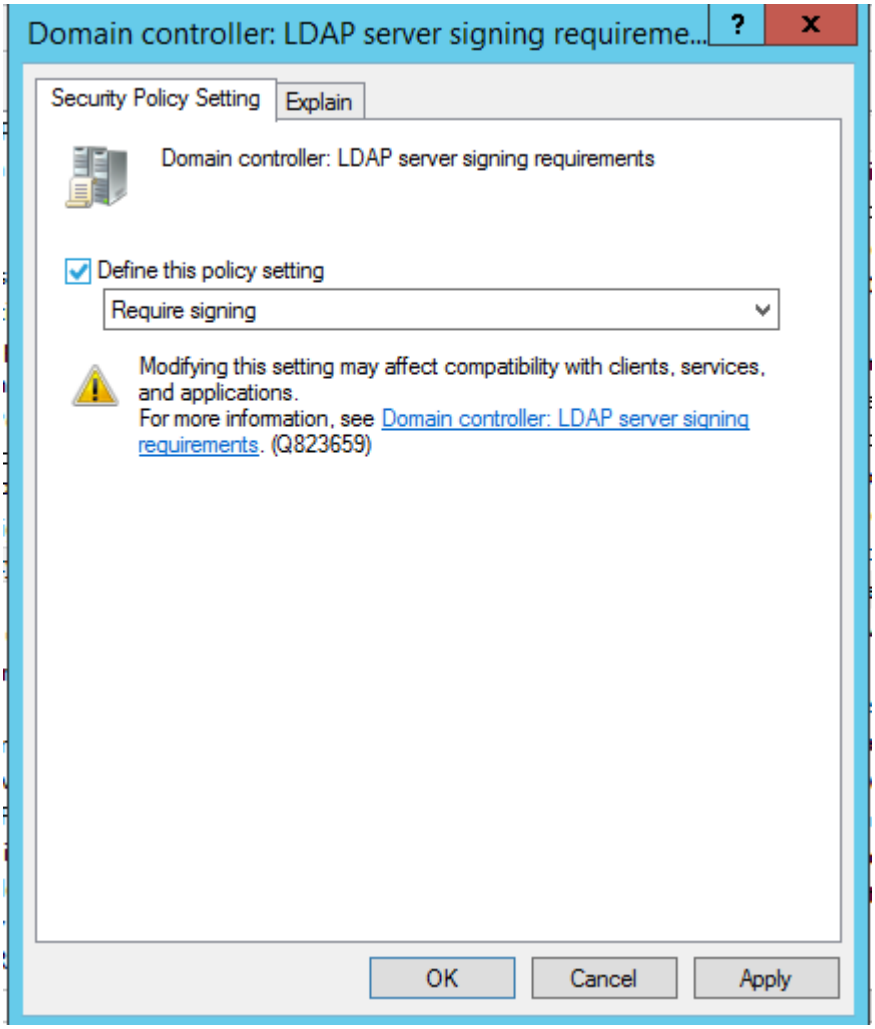
Pilih domain controller -> Pilih Default Domain controller Policy:



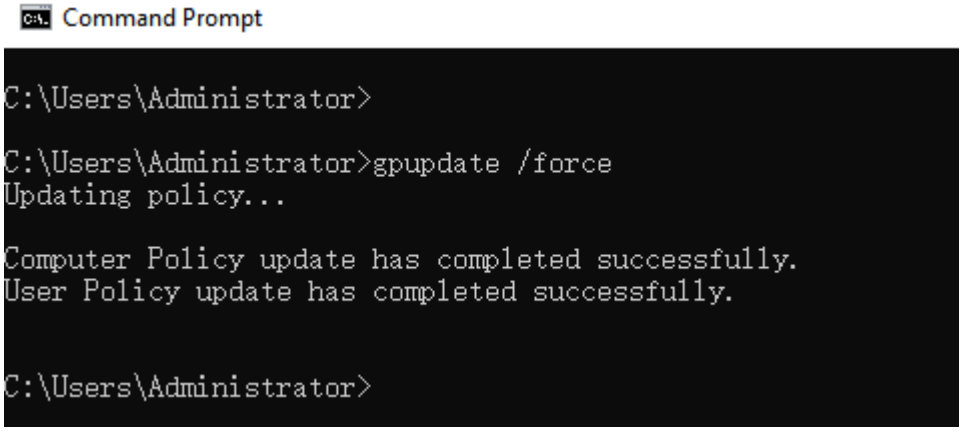
Klik Kanan Edit dan buka group management editor:



Ubah pengaturan ke Required signing.



Setelah dikonfigurasi, CMD run gpupdate /force untuk push group policy.



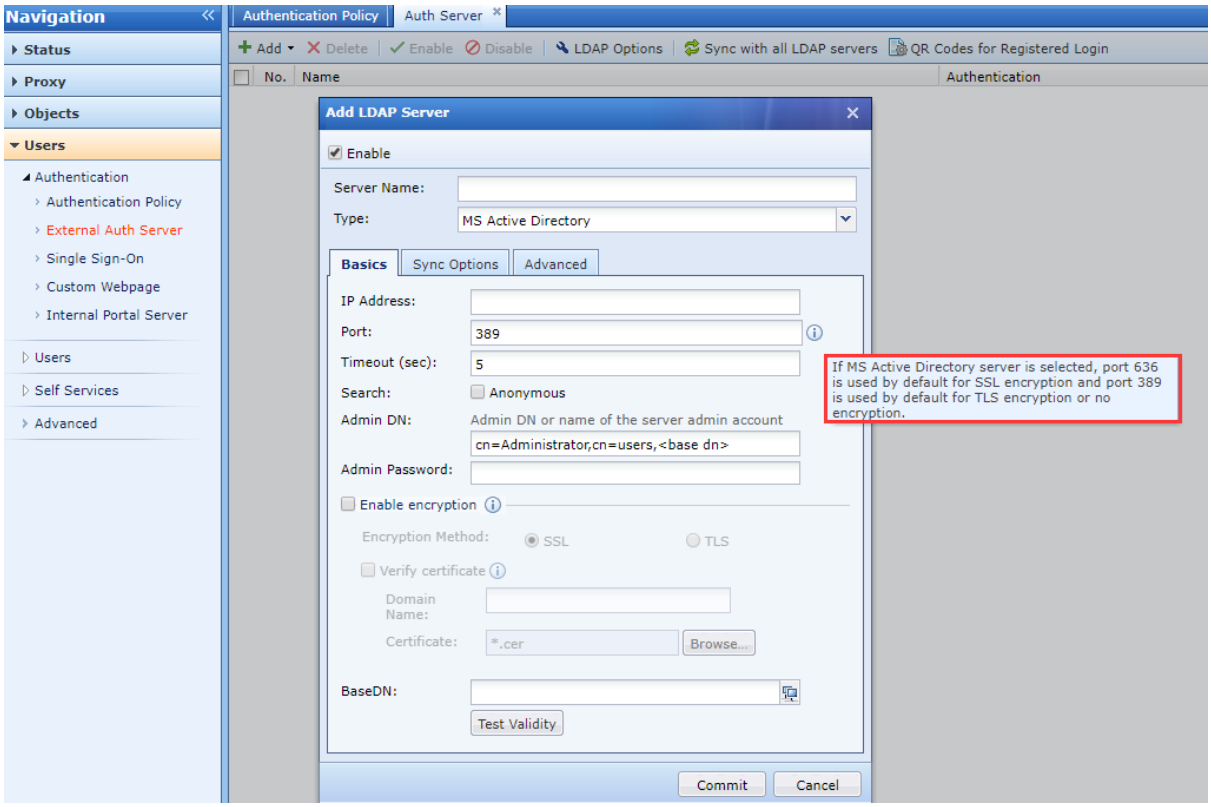
4.4 AD Konfigurasi pada IAM

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

4.4.1 Deskripsi Autentikasi Port

Seperti yang ditunjukkan pada gambar, the LDAP server dikonfigurasi di external authentication server untuk terhubung dengan Microsoft AD domain:

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

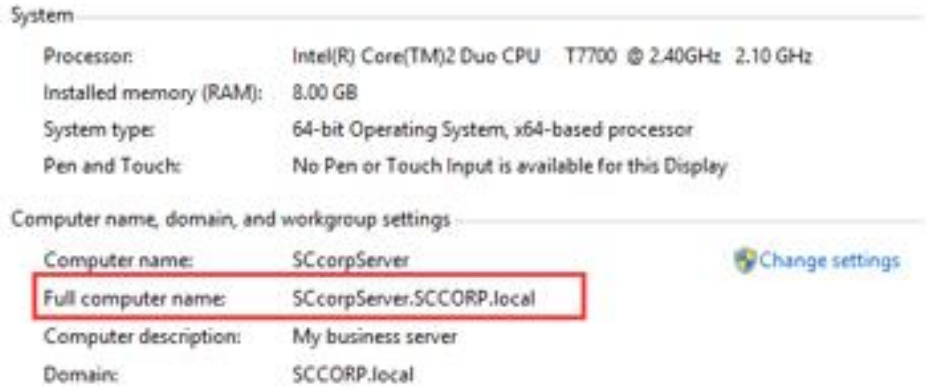


4.4.2 Aktifkan Enkripsi

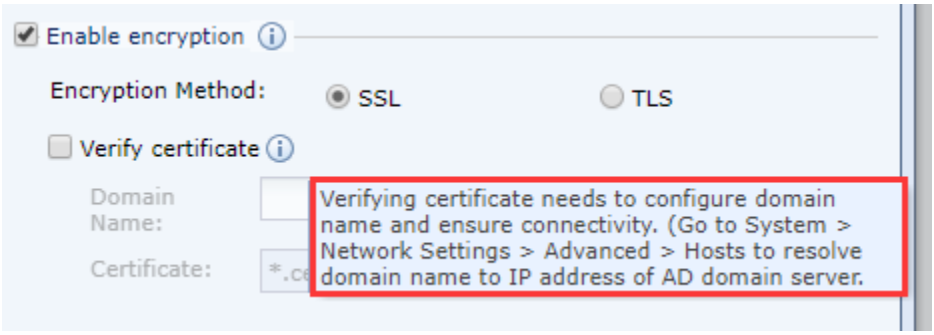
Seperti yang ditunjukkan pada gambar di bawah ini:

- LDAP server dapat dikonfigurasi untuk tidak mengaktifkan enkripsi. Dalam skenario ini, persyaratan LDAP server signing tidak diaktifkan di Microsoft AD domain.
- Jika AD domain telah dikonfigurasi untuk mengaktifkan persyaratan LDAP server signing, maka enkripsi harus diaktifkan di sini . Metode enkripsi dapat dipilih sendiri, dan autentikasi port dapat dimodifikasi sesuai dengan metode enkripsi yang dipilih seperti dijelaskan di atas.
- Fungsi verifikasi sertifikat dapat dimatikan, dan itu tidak akan mempengaruhi koneksi dengan AD domain dengan persyaratan server signing.
- Jika fungsi verifikasi sertifikat diaktifkan, Anda perlu mengkonfigurasi domain name dan import certificare 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 mendapatkan field, seperti yang ditunjukkan pada gambar berikut:



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



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