SANGFOR

IAM
Password-based authentication with AD

Version 12.0.42

Change Log

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

CONTENT

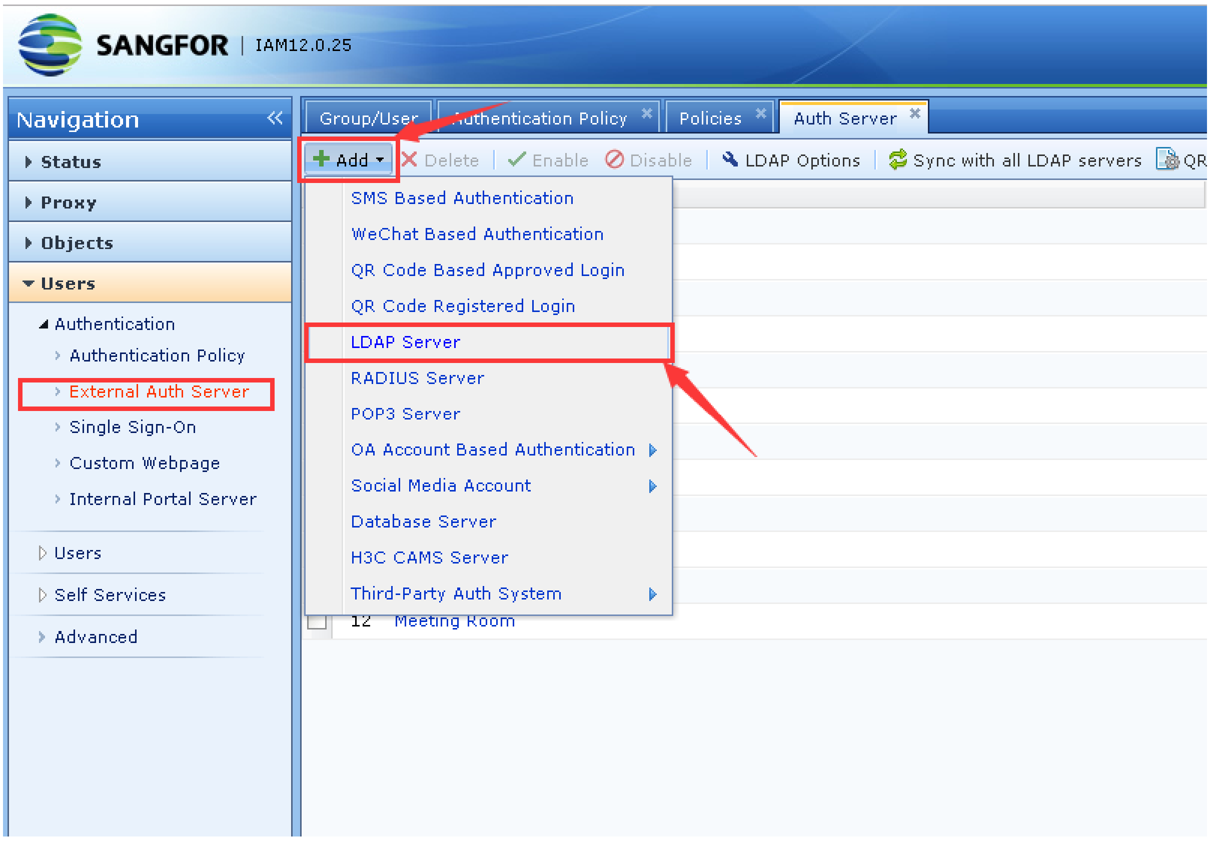
Chapter 1 Content Requirement

1. IAM device (version 12.0.42 or above), a PC, and an AD domain server.
2. Deploy the network environment, make sure all the devices and AD domain server can connect to IAM.

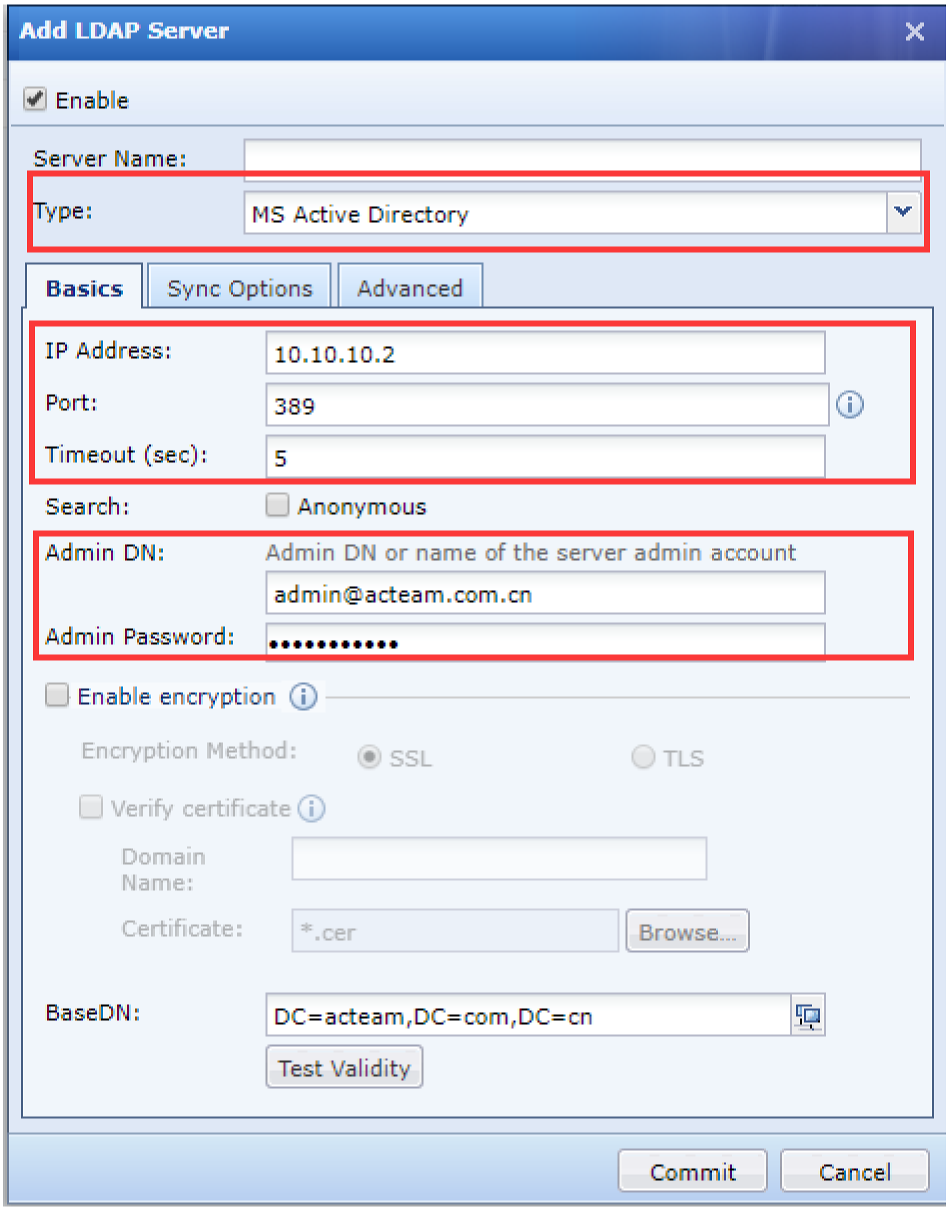
Chapter 2 Configuration and Screenshots

2.1 LDAP Server Configuration

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



2. Configure LDAP server information.



☑ Enable

Server Name:

Type: MS Active Directory

IP Address: 10.10.10.2

Port: 389

Timeout (sec): 5

Search: ☐ Anonymous

Admin DN: Admin DN or name of the server admin account

admin@acteam.com.cn

Admin Password: •••••••••••

☐ Enable encryption

Encryption Method: ● SSL ○ TLS

☐ Verify certificate

Domain Name:

Certificate: *.cer

BaseDN: DC=acteam,DC=com,DC=cn

[IP Address]: IP address of LDAP server.

[Authentication port]: Port which connected to LDAP server, for example, AD domain is 389.

[Timeout]: Set the timeout period of the authentication request. After the system forwards the authentication request to the LDAP server, if there is no response after this time, the authentication is considered to be invalid. If the network between the device and the LDAP server is slow, you can try Set the timeout to be larger (for example, 10 seconds).

[Search]: This option is available when the LDAP server supports anonymous search.

[Admin DN]: User account used for querying and synchronizing to the LDAP server; for example, the account is: administrator, the domain name is sangfor.com, then the format is: username@domain, administrator@sangfor.com.cn

[Admin Password]: The password corresponding to the user who is used to bind the server.

[BaseDN]: Specify the starting point of the domain search path, which determines the effective scope of the LDAP rule. If the user is outside the specified BaseDN, the user cannot be authenticated by the external server, and the configured policy will not take effect for the user. Therefore, you can use BaseDN to divide the area of different administrators.

[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.

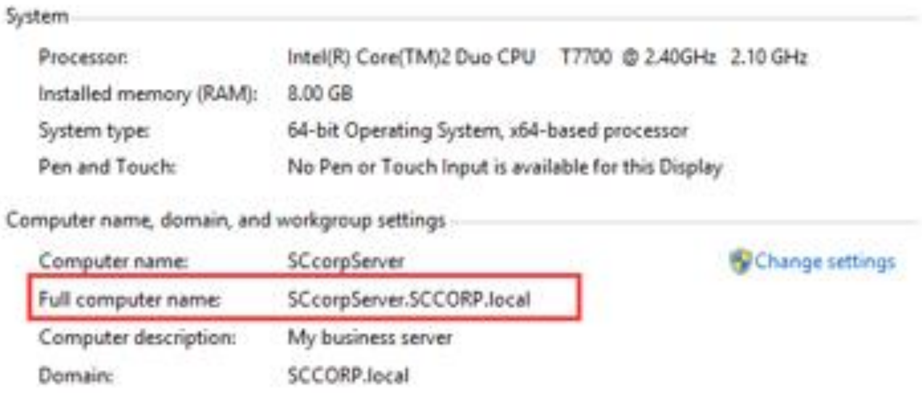
Official configuration by Microsoft：

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.



System

Processor: Intel(R) Core(TM)2 Duo CPU T7700 @ 2.40GHz 2.10 GHz

Installed memory (RAM): 8.00 GB

System type: 64-bit Operating System, x64-based processor

Pen and Touch: No Pen or Touch Input is available for this Display

Computer name, domain, and workgroup settings

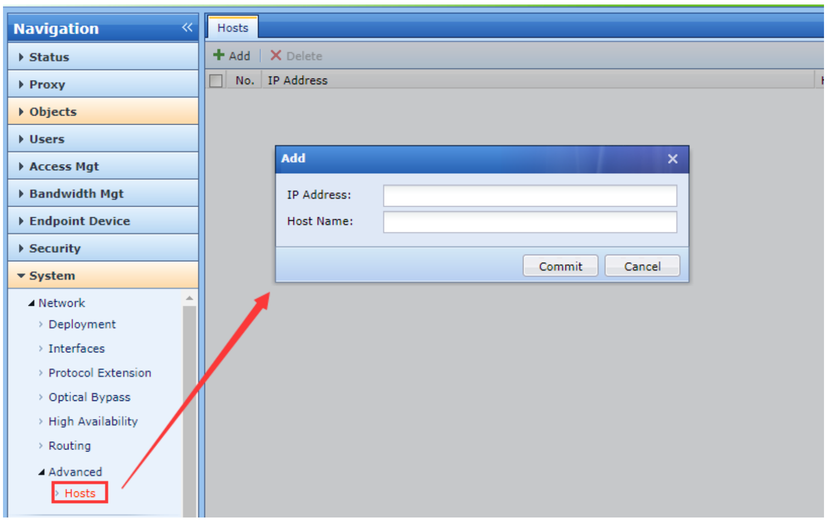
Computer name: SCcorpServer

Full computer name: SCcorpServer.SCCORP.local

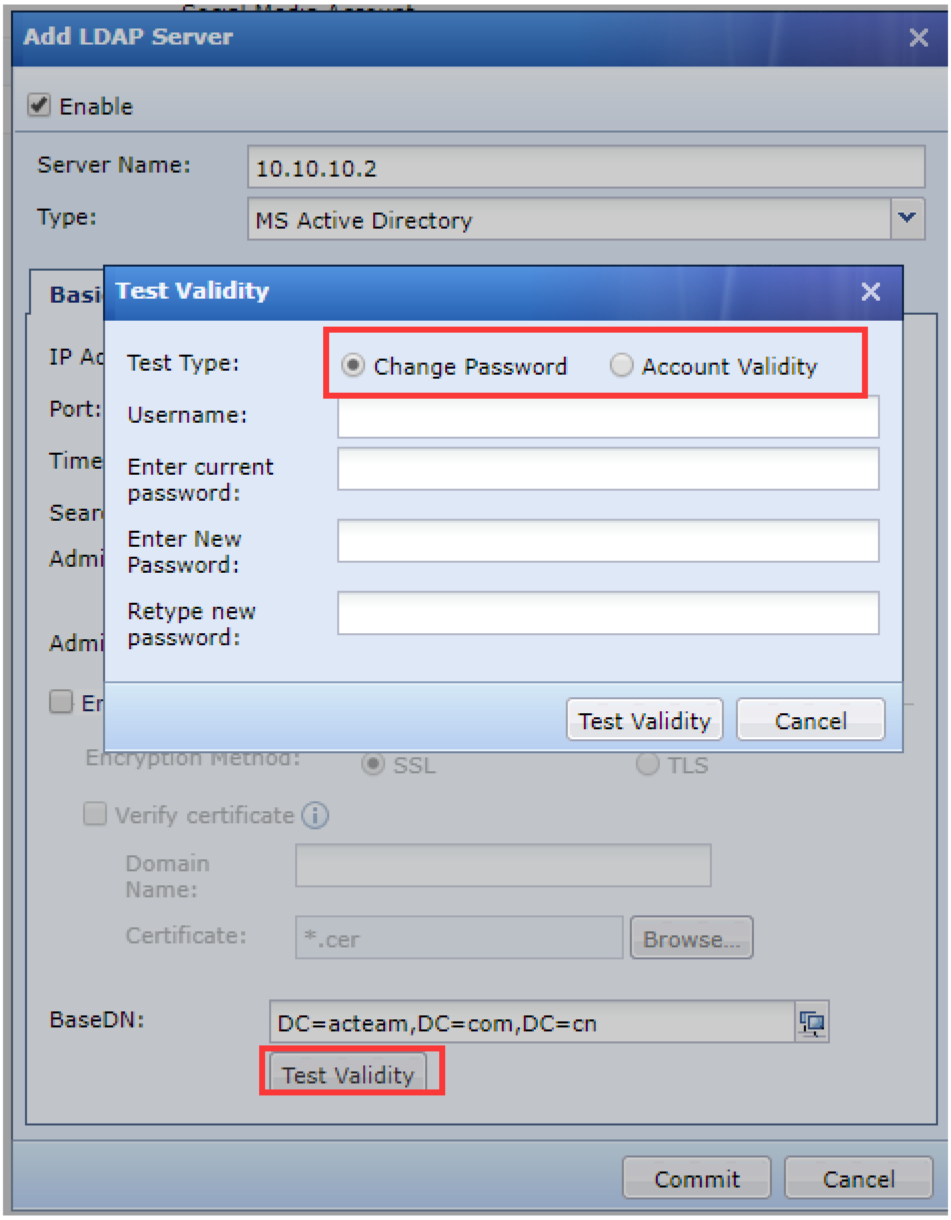
Computer description: My business server

Domain: SCCORP.local

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



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



☑ Enable

Server Name: 10.10.10.2

Type: MS Active Directory

Test Validity

Test Type: ● Change Password ○ Account Validity

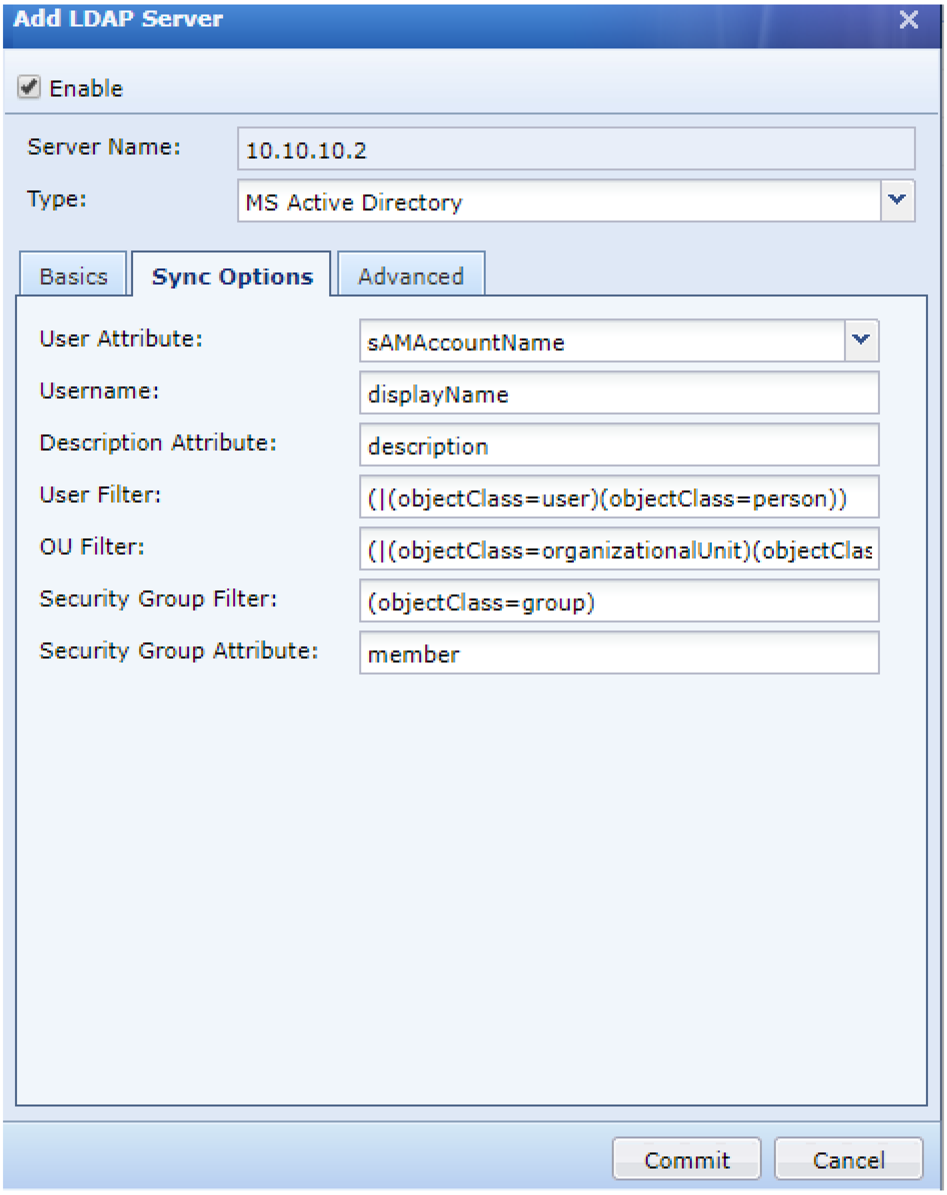
BaseDN: DC=acteam,DC=com,DC=cn

Test Validity

[Change Password]: If the AD domain account is checked for first time authentication and the password can be changed, then the password can be changed directly here.

[Account Validity]: Tests whether the IAM device can communicate directly with the AD domain and verify that the account is valid.

4. Edit **[sync options]** (If there is no special requirement, it is not recommended to edit and modify, keep the default).



☑ Enable

Server Name: 10.10.10.2

Type: MS Active Directory

User Attribute: sAMAccountName

Username: displayName

Description Attribute: description

User Filter: (|(objectClass=user)(objectClass=person))

OU Filter: (|(objectClass=organizationalUnit)(objectClas

Security Group Filter: (objectClass=group)

Security Group Attribute: member

[User Attribute]: Specifies the attribute field on the LDAP server that uniquely identifies the user. For example, the sAMAccountName attribute on the AD domain identifies the user, and on the Novell LDAP, the uid attribute identifies the user.

[Username]: Specifies the attribute field on the LDAP server that uniquely identifies the user display name. For example, the displayName attribute on the AD domain identifies the user's display name.

[Description Attribute]: Specifies the attribute field on the LDAP server that uniquely identifies the user description. For example, the description attribute on the AD domain identifies the user's description.

[User Filter]: Specifies the user filtering condition of the LDAP server. That is, you can determine whether a node is a user. For example, you can filter whether a node is a user by filling in "(|(objectClass=user)(objectClass=person))" .

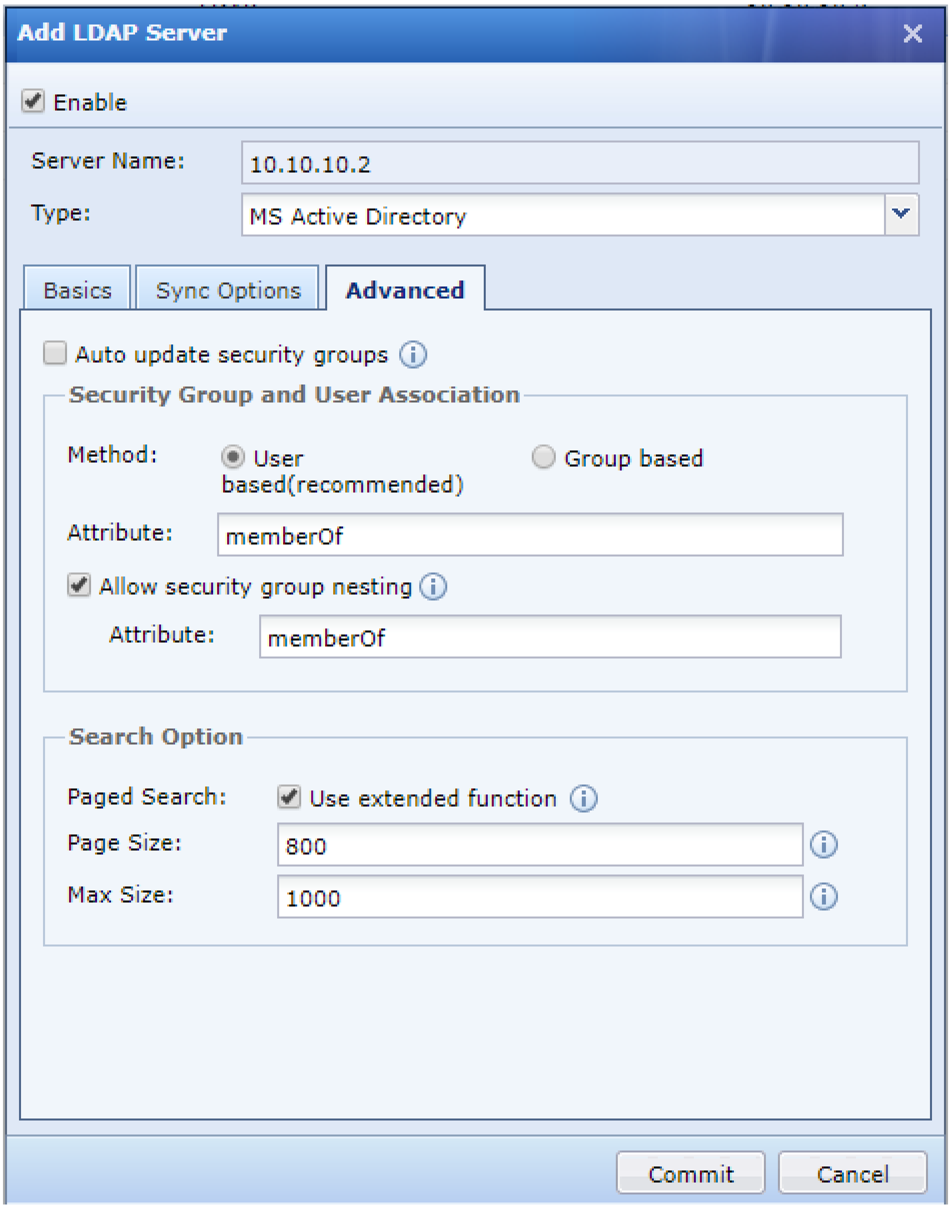
[OU Filter]: Specifies the organizational unit filter condition of the LDAP server, that is, whether the node can be an organizational unit by using this condition. For example, the AD domain can be filled in by "(|(objectClass=organizationalUnit)(objectClass=organization)(objectClass=domain)(objectClass =domainDNS)(objectClass=container))" to filter whether a node is an organizational unit.

[Security Group Filter]: Specify the (security) group filter condition of the LDAP server (Note: for the AD domain, here is the security group, for the non-AD domain, here is the group), that is, through this condition, it can be determined Whether the node is a (secure) group, for example, the AD domain can be used to filter whether a node is a security group by filling in "(objectClass=group)".

[Security Group Attribute]: Specifies which attribute on the AD domain server identifies the member list of the security group. This attribute takes effect only when the LDAP server is an AD domain. If there is no special case in this field, you can usually fill in the member.

When the server type selects "MS Active Directory", the above parameters are set. Generally, the default parameters can be used. If the server is other types of LDAP, it needs to be adjusted according to the actual situation, so that the device can read the correct LDAP.

5. Edit **[Advance]** configuration.



Add LDAP Server

☑ Enable

Server Name: 10.10.10.2

Type: MS Active Directory

☐ Auto update security groups

Security Group and User Association

Method: ● User based(recommended) ○ Group based

Attribute: memberOf

☑ Allow security group nesting

Attribute: memberOf

Search Option

Paged Search: ☑ Use extended function

Page Size: 800

Max Size: 1000

[Auto update security groups]: After checking, the LDAP server will be requested in real time to synchronize the contents of the required synchronization to the local, but will increase the pressure on the LDAP server. This option is only valid for the AD domain.

[Security Group and User Association]: The default configuration is recommended here.

[Method]: You can choose "users to find (recommended)" or "group to find users". If the user has an attribute on the LDAP server that holds the group to which it belongs, you can select "User Group (Recommended)" because this method will provide better performance and reduce the performance pressure on the LDAP server. If there is no information stored between the user and the group on the LDAP server, only the group saves the user. In this case, you need to check the group to find the user.

[Attribute]: If the "User based" mode is selected, this field needs to fill in the group on the LDAP server or the user saves the attributes of its parent group. For example, the memberOf attribute on the AD domain identifies the parent group of a node, so when searching, the memberOf attribute is used to search for its parent group. If "Group based" is selected, this field needs to fill in the attributes of the group save subuser on the LDAP server. For example, the member attribute on the AD domain identifies a sub-user of a group, so when searching, the member attribute is used to search for a sub-user of a group.

[Allow security group nesting]: The check box determines whether the configuration (security) group is valid for the users under the group, or whether the users and subgroups under the group are recursive. If you select this field, the user and sub-groups of the corresponding (secure) group will be recursively effective. If unchecked, it means that only the subordinate users in the configured (secure) group are valid, and all subgroups are ignored.

[Nesting Attribute]: Nested properties can only be filled after "Allow security group nesting" is checked. This option indicates which attribute is used by the group that needs to be searched for when recursively looking up. If the "User based" mode is selected, this field only needs to be consistent with the "Associated Properties". If "Group based" is selected, this field needs to fill in the attributes of the group save subgroup on the LDAP server. For example, the member attribute on the AD domain identifies all subgroups of a group, so when searching, the member attribute is used to search all subgroups of a group.

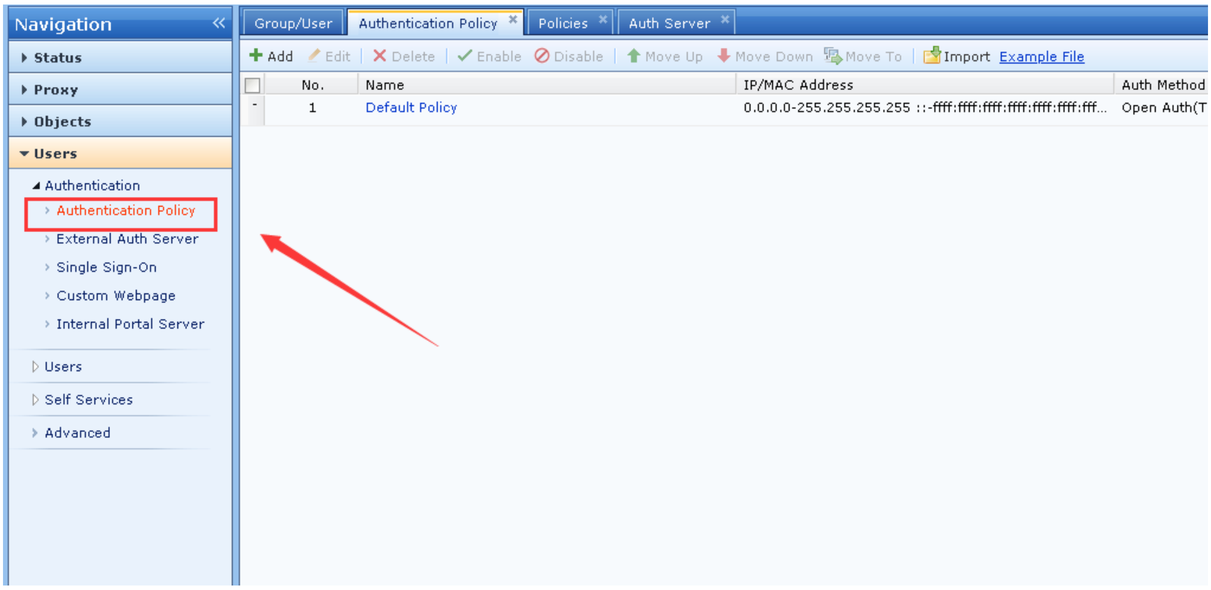
[Page search]: To search the LDAP server using the extension API, it is recommended to keep the default configuration.

[Page size]: The size returned when LDAP is paged, 0 means no limit, it is recommended to keep the default configuration.

[Max size]: The size limit option when synchronizing LDAP, it is recommended to keep the default configuration.

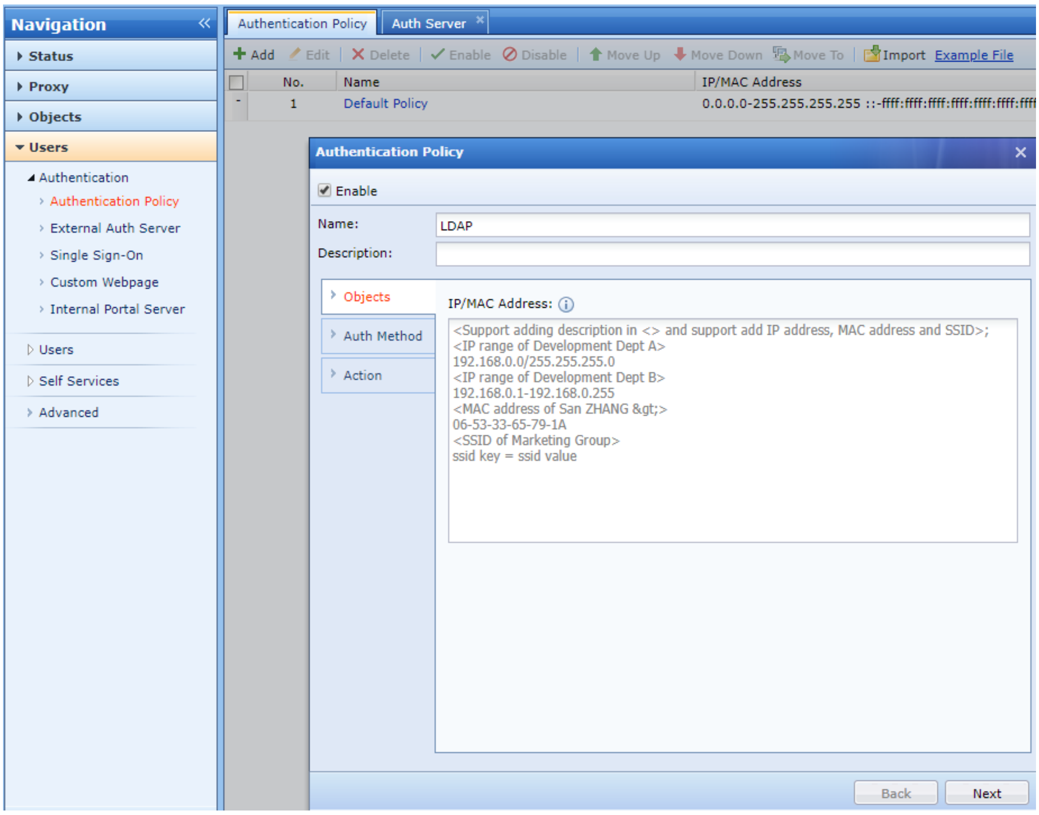
2.2 User Authentication Configuration

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



No.	Name	IP/MAC Address	Auth Method
1	Default Policy	0.0.0.0-255.255.255.255 ::-ffff:ffff:ffff:ffff:ffff:ffff:fff...	Open Auth(T

2. **Add** > **Authentication Policy** - It is recommended to test the process at the beginning of the test for a single address. After the test is successful, gradually expand the test range.



☑ Enable

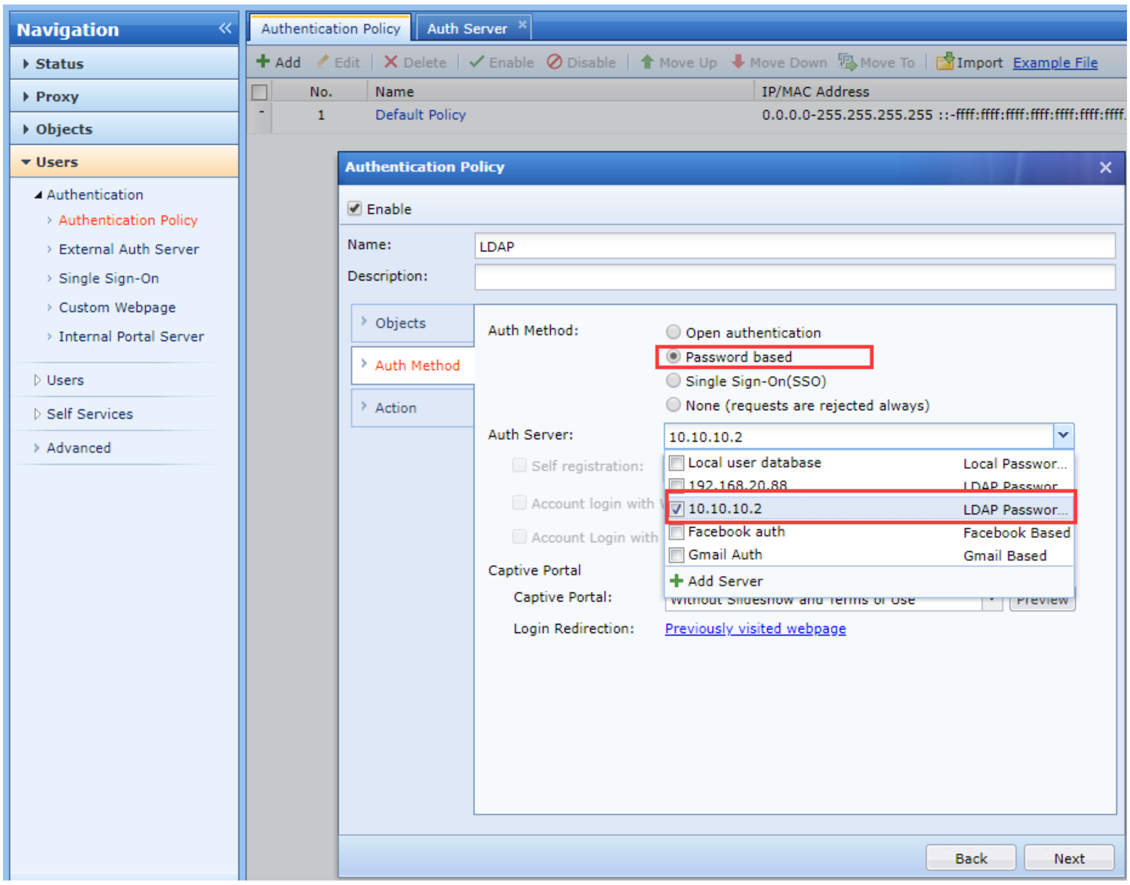
Name: LDAP

Description:

IP/MAC Address:

<Support adding description in <> and support add IP address, MAC address and SSID>;
<IP range of Development Dept A>
192.168.0.0/255.255.255.0
<IP range of Development Dept B>
192.168.0.1-192.168.0.255
<MAC address of San ZHANG &gt;>
06-53-33-65-79-1A
<SSID of Marketing Group>
ssid key = ssid value

3. **Authentication method**: Choose authentication method: Password based. Auth server: Select the - LDAP domain server created in the external auth server.



No.	Name	IP/MAC Address
1	Default Policy	0.0.0.0-255.255.255.255 ::-ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Authentication Policy

☑ Enable

Name: LDAP

Description:

Auth Method:
○ Open authentication
● Password based
○ Single Sign-On(SSO)
○ None (requests are rejected always)

Auth Server: 10.10.10.2

□ Local user database	Local Passwor...
□ 192.168.20.88	LDAP Passwor
☑ 10.10.10.2	LDAP Passwor...
□ Facebook auth	Facebook Based
□ Gmail Auth	Gmail Based

□ Self registration:

□ Account login with

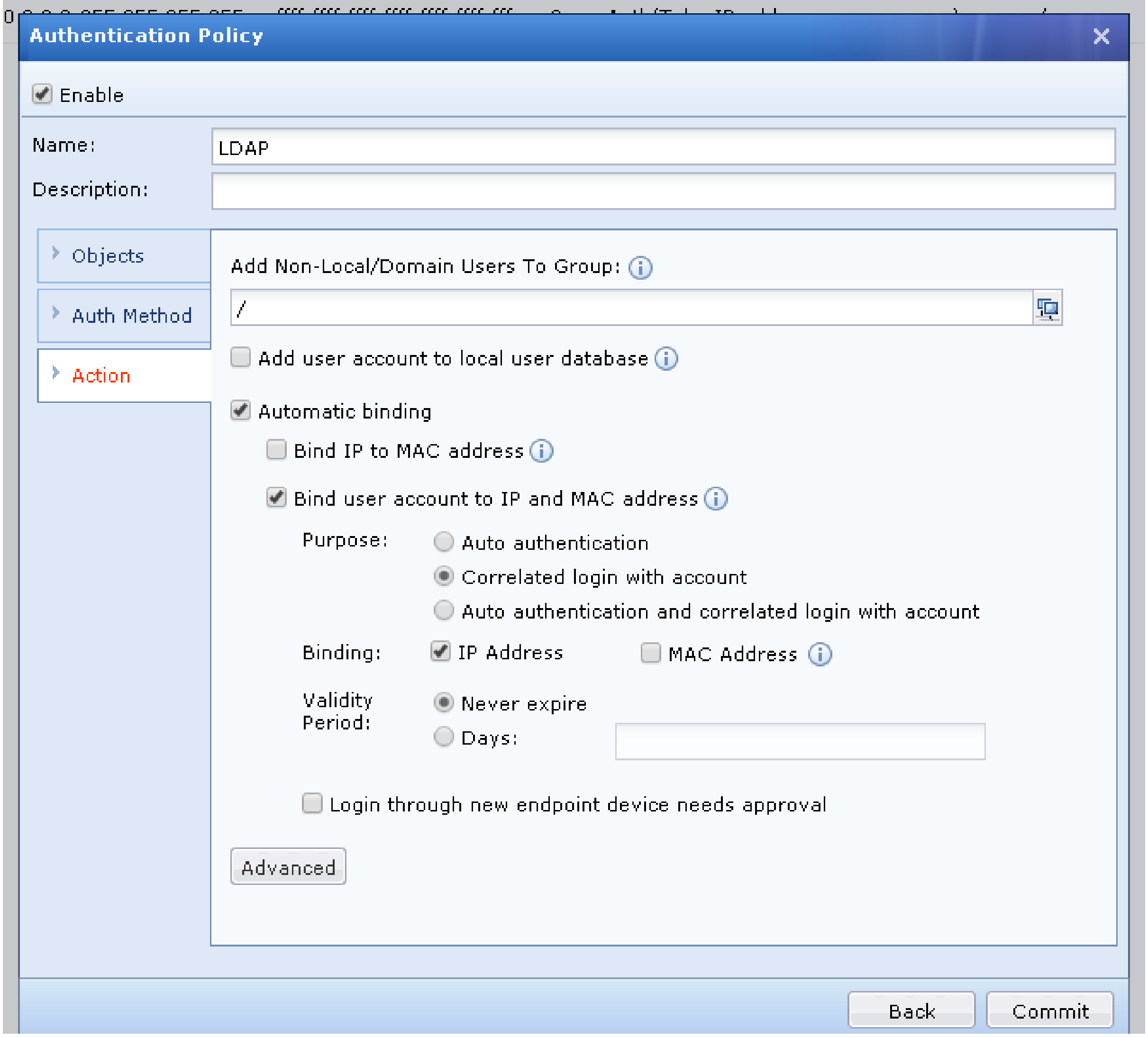
□ Account Login with

Captive Portal

Captive Portal: Without Slideshow and Terms of Use

Login Redirection: Previously visited webpage

4. Action configuration requirement after authentication process.



Authentication Policy

☑ Enable

Name: LDAP

Description:

- Objects
- Auth Method
- Action

Add Non-Local/Domain Users To Group: /

☐ Add user account to local user database

☑ Automatic binding

☐ Bind IP to MAC address

☑ Bind user account to IP and MAC address

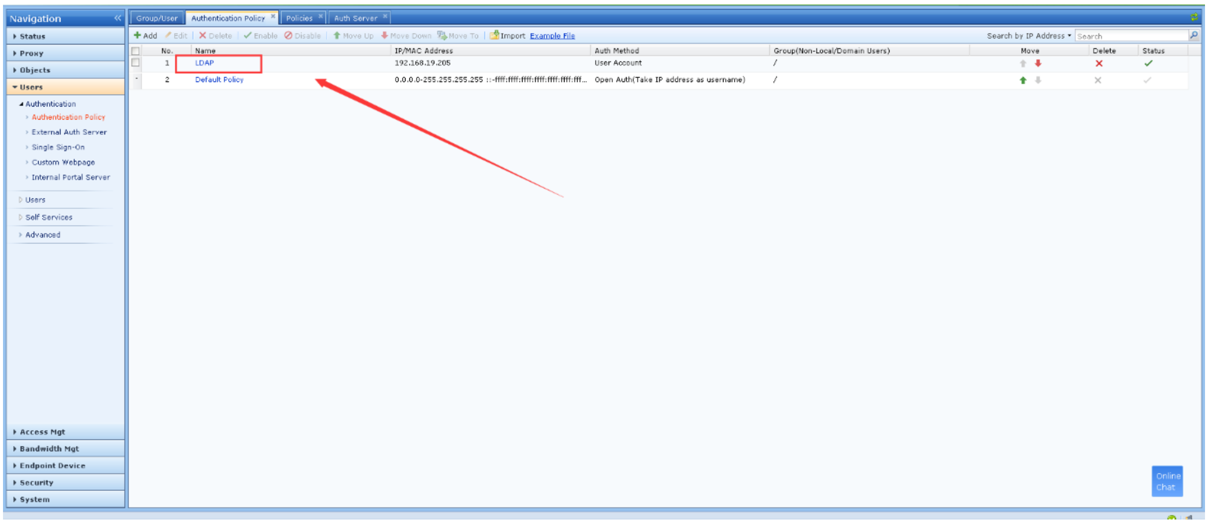
Purpose: ○ Auto authentication ● Correlated login with account ○ Auto authentication and correlated login with account

Binding: ☑ IP Address ☐ MAC Address

Validity Period: ● Never expire ○ Days:

☐ Login through new endpoint device needs approval

5. You can see the new policy in the authentication policy interface.

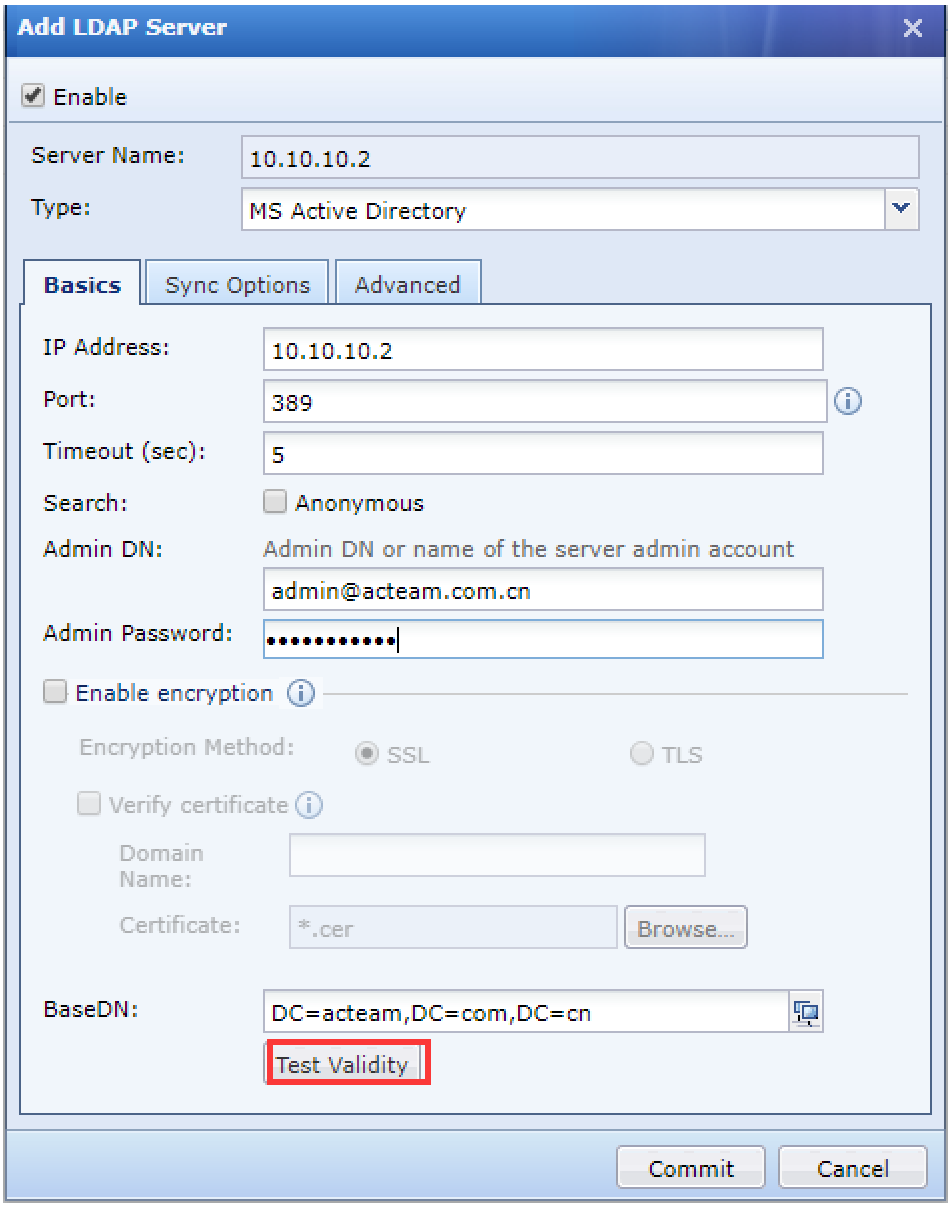


No.	Name	IP/MAC Address	Auth Method	Group(Non-Local/Domain Users)	Move	Delete	Status
1	LDAP	192.168.19.205	User Account	/	↑ ↓	×	✓
2	Default Policy	0.0.0.0-255.255.255.255 ::-ffff:ffff:ffff:ffff:ffff:ffff:fff...	Open Auth(Take IP address as username)	/	↑ ↓	×	✓

Chapter 3 Precaution

1. When configuring the external authentication server administrator account and password, it is

recommended to click - [test validity] to ensure that it is available. as the picture shows:



Add LDAP Server

☑ Enable

Server Name: 10.10.10.2

Type: MS Active Directory

IP Address: 10.10.10.2

Port: 389

Timeout (sec): 5

Search: □ Anonymous

Admin DN: Admin DN or name of the server admin account

admin@acteam.com.cn

Admin Password: ●●●●●●●●●●●

□ Enable encryption

Encryption Method: ● SSL ○ TLS

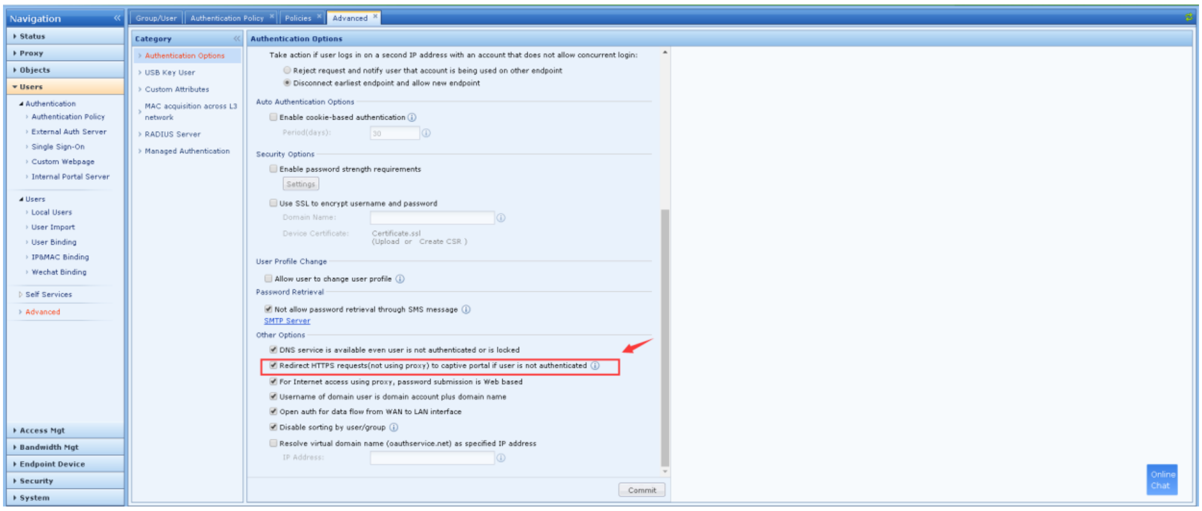
□ Verify certificate

Domain Name:

Certificate: *.cer Browse...

BaseDN: DC=acteam,DC=com,DC=cn

2. The client opens the web page to pop up the authentication page. If it is domain URL link to open the link, you need to be able to resolve the domain name and open the URL of http. If you need to open the URL of https, you need to go to the authentication page. You need to select the authentication option. The options on the image below:



Authentication Options

Take action if user logs in on a second IP address with an account that does not allow concurrent login:

○ Reject request and notify user that account is being used on other endpoint

● Disconnect earliest endpoint and allow new endpoint

Auto Authentication Options

□ Enable cookie-based authentication

Period(days): 30

Security Options

□ Enable password strength requirements

Settings

□ Use SSL to encrypt username and password

Domain Name:

Device Certificate: Certificate.ssl (Upload or Create CSR)

User Profile Change

□ Allow user to change user profile

Password Retrieval

☑ Not allow password retrieval through SMS message

SMTP Server

Other Options

☑ DNS service is available even user is not authenticated or is locked

☑ Redirect HTTPS requests(not using proxy) to captive portal if user is not authenticated

☑ For Internet access using proxy, password submission is Web based

☑ Username of domain user is domain account plus domain name

☑ Open auth for data flow from WAN to LAN interface

☑ Disable sorting by user/group

□ Resolve virtual domain name (oauthservice.net) as specified IP address

IP Address:

3. If the signing requirement is 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 4 Appendix A: LDAPS Configuration Guide

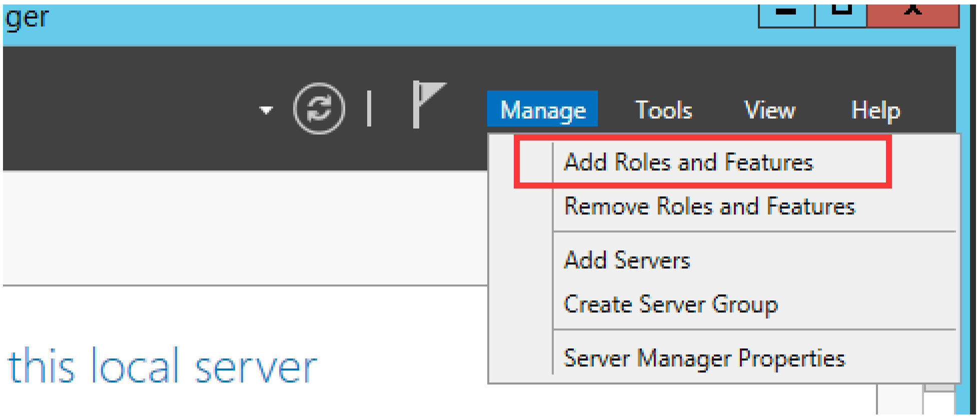
4.1 Background

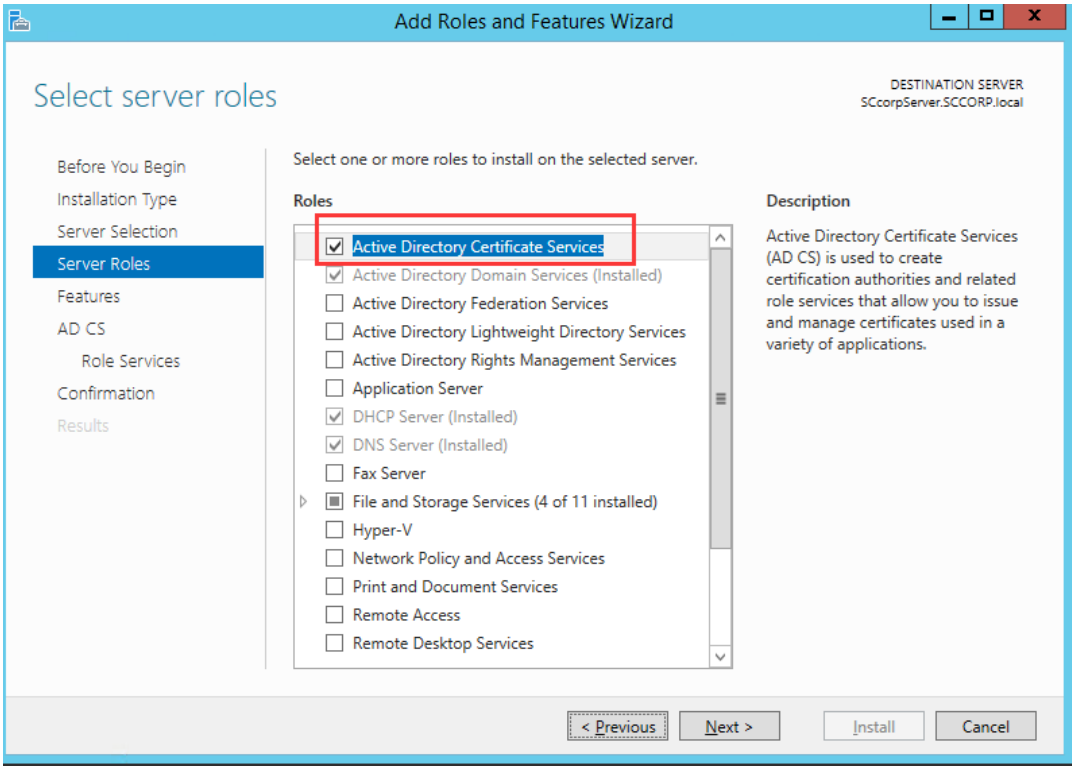
In September 2019, Microsoft announced in the security bulletin [ADV190023 | Microsoft Guidance for Enabling LDAP Channel Binding and LDAP Signing] that LDAP channel binding and LDAP signing will be enabled on the Active Directory server through the security update method (KB patch) in mid-January 2020. 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.

4.2 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 server roles

DESTINATION SERVER
SCcorpServer.SCCORP.local

Select one or more roles to install on the selected server.

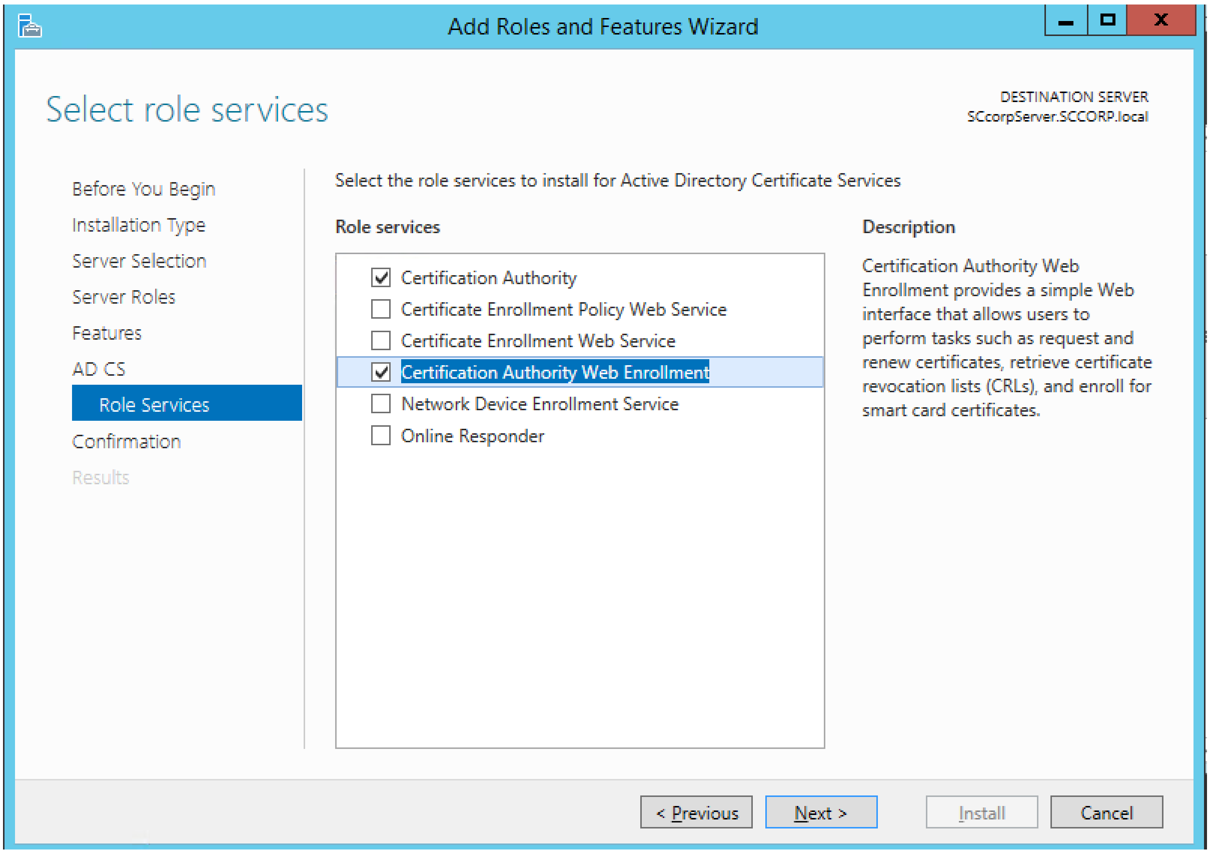
Roles

- ☑ 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.

Select Certificate Authority and Certificate Authority Web Enrollment:



Add Roles and Features Wizard

Select role services

DESTINATION SERVER
SCcorpServer.SCCORP.local

Select the role services to install for Active Directory Certificate Services

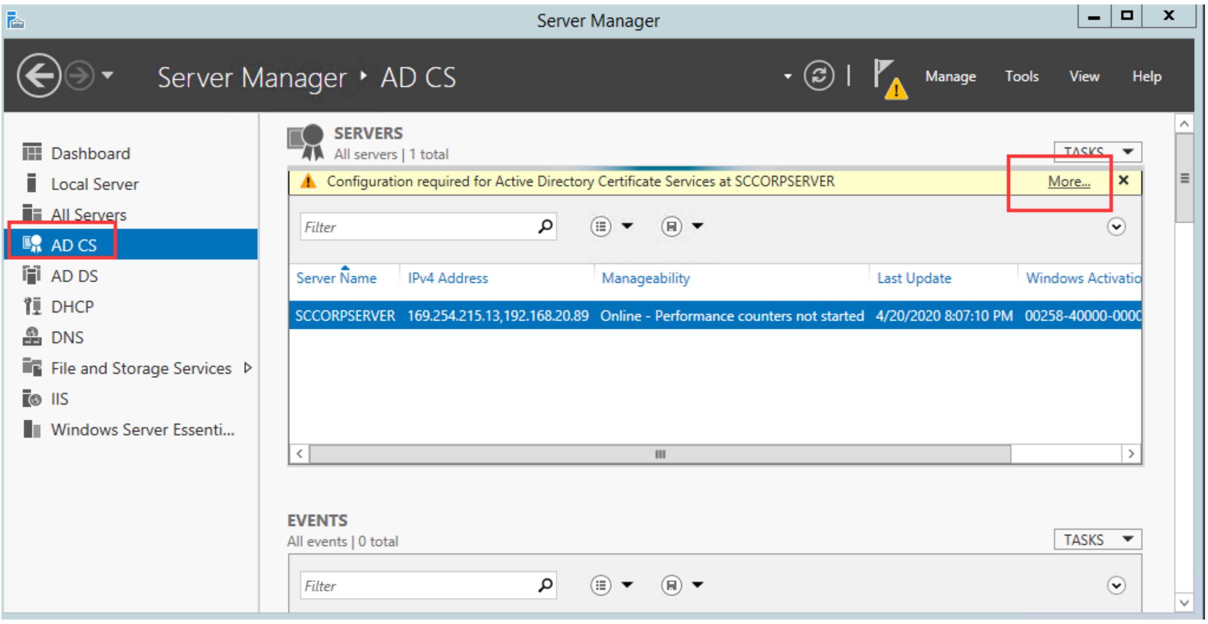
Role services

- ☑ Certification Authority
- □ Certificate Enrollment Policy Web Service
- □ Certificate Enrollment Web Service
- ☑ Certification Authority Web Enrollment
- □ Network Device Enrollment Service
- □ Online Responder

Description

Certification Authority Web Enrollment provides a simple Web interface that allows users to perform tasks such as request and renew certificates, retrieve certificate revocation lists (CRLs), and enroll for smart card certificates.

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



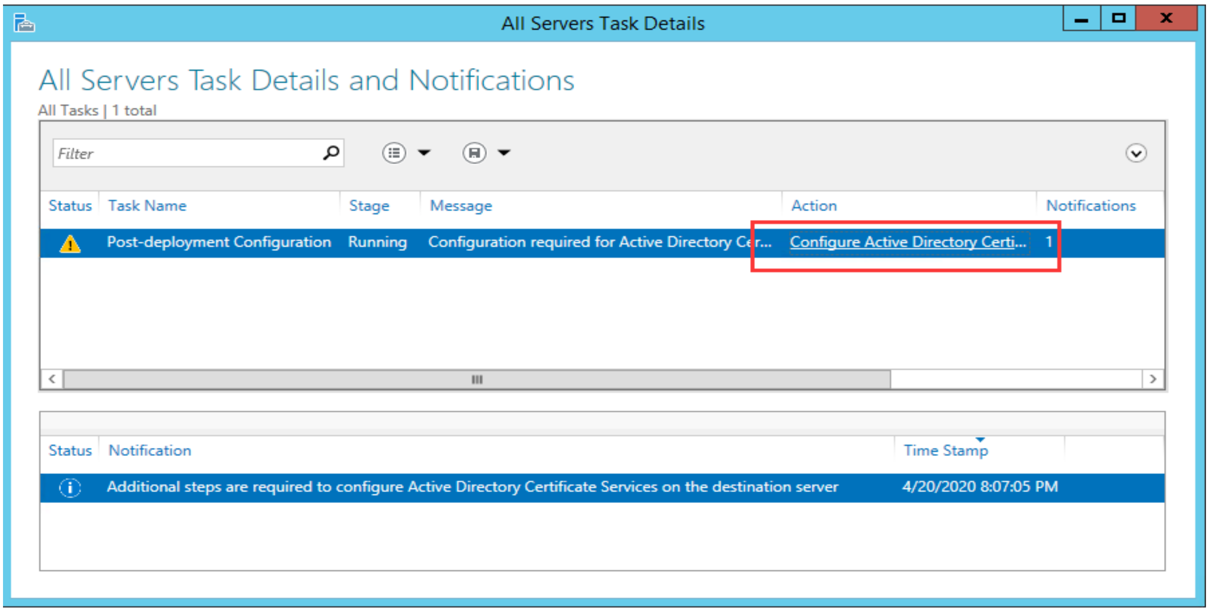
Server Manager

SERVERS
All servers | 1 total

⚠ Configuration required for Active Directory Certificate Services at SCCORPSERVER More... ✕

Server Name	IPv4 Address	Manageability	Last Update	Windows Activatio
SCCORPSERVER	169.254.215.13,192.168.20.89	Online - Performance counters not started	4/20/2020 8:07:10 PM	00258-40000-000

EVENTS
All events | 0 total



All Servers Task Details

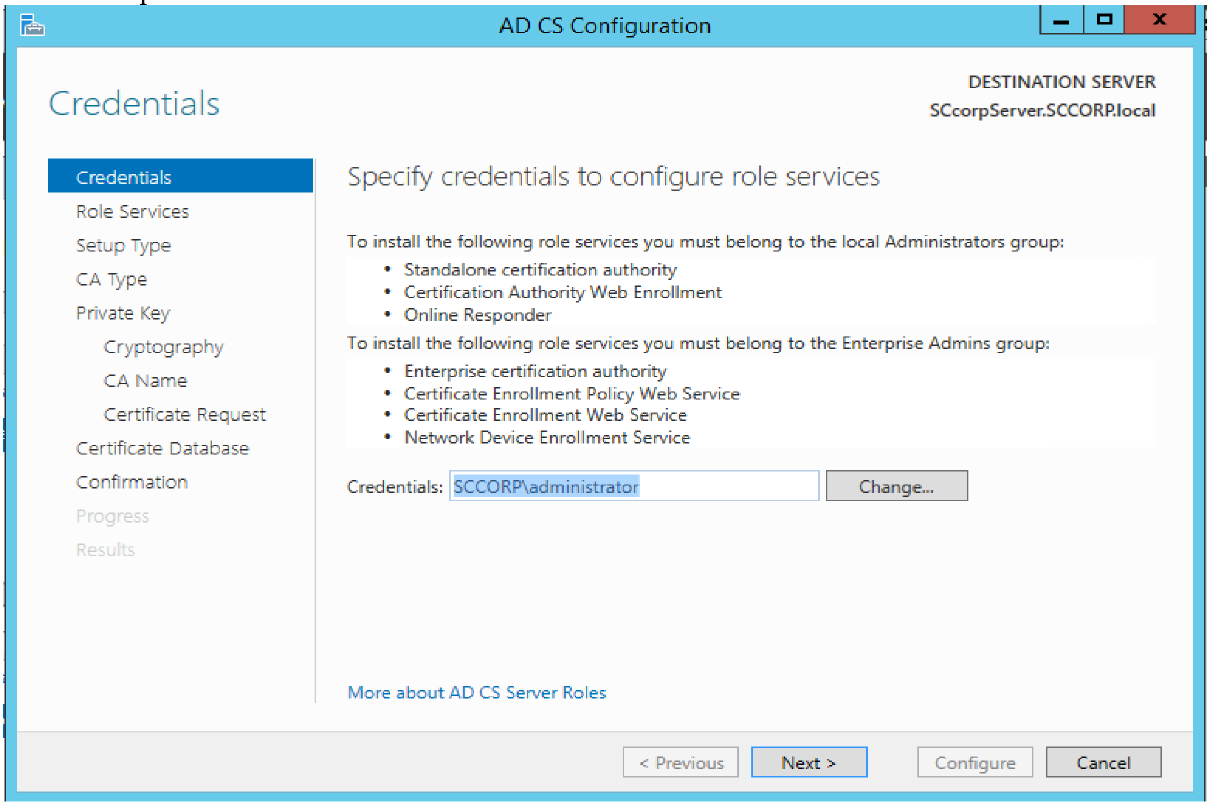
All Servers Task Details and Notifications

All Tasks | 1 total

Status	Task Name	Stage	Message	Action	Notifications
⚠	Post-deployment Configuration	Running	Configuration required for Active Directory Cer...	Configure Active Directory Certi...	1

Status	Notification	Time Stamp
ⓘ	Additional steps are required to configure Active Directory Certificate Services on the destination server	4/20/2020 8:07:05 PM

Select Enterprise CA:



AD CS Configuration

Credentials

DESTINATION SERVER
SCcorpServer.SCCORP.local

Specify credentials to configure role services

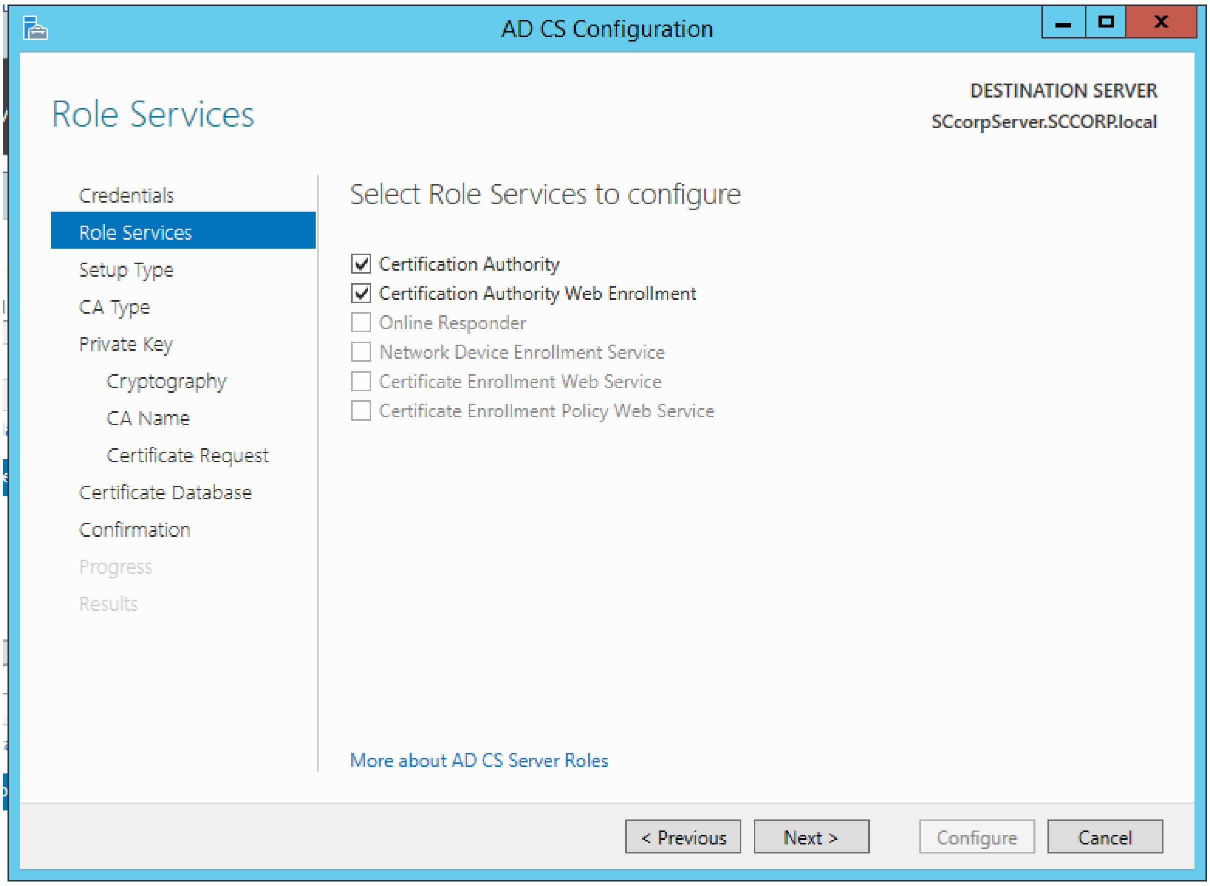
To install the following role services you must belong to the local Administrators group:

- 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: SCCORP\administrator

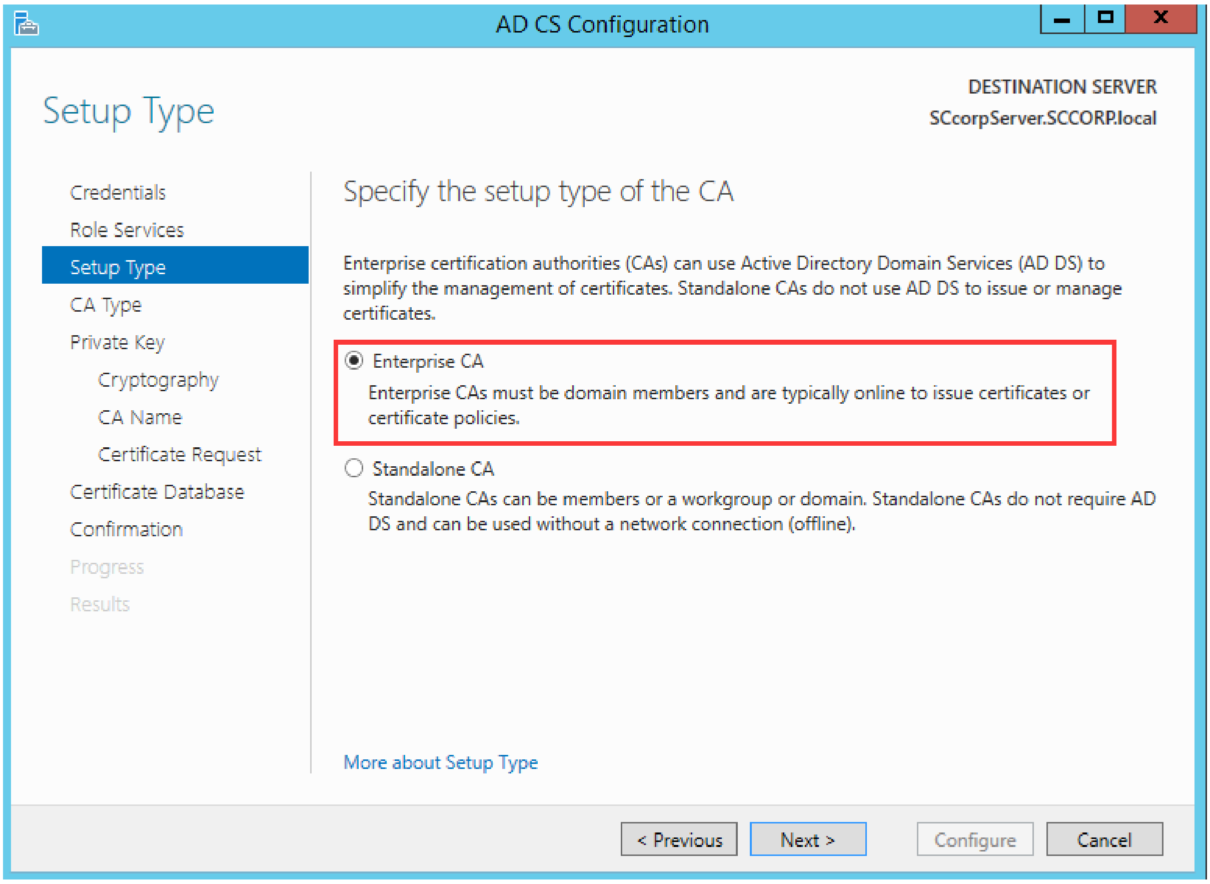


Role Services

DESTINATION SERVER
SCcorpServer.SCCORP.local

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



Setup Type

DESTINATION SERVER
SCcorpServer.SCCORP.local

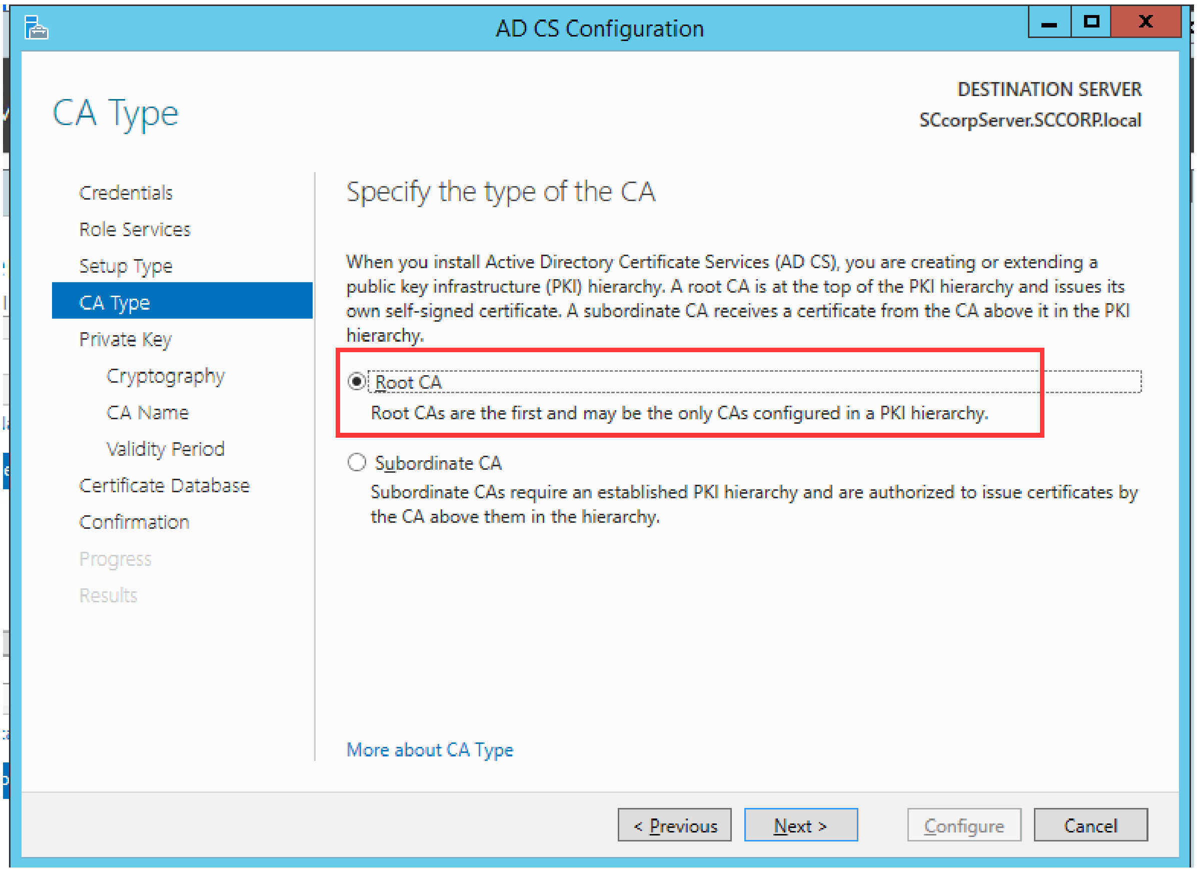
Specify the setup type of the CA

Enterprise certification authorities (CAs) can use Active Directory Domain Services (AD DS) to simplify the management of certificates. Standalone CAs do not use AD DS to issue or manage certificates.

● Enterprise CA
Enterprise CAs must be domain members and are typically online to issue certificates or certificate policies.

○ Standalone CA
Standalone CAs can be members or a workgroup or domain. Standalone CAs do not require AD DS and can be used without a network connection (offline).

Select Root CA and create New Private Key:



AD CS Configuration

CA Type

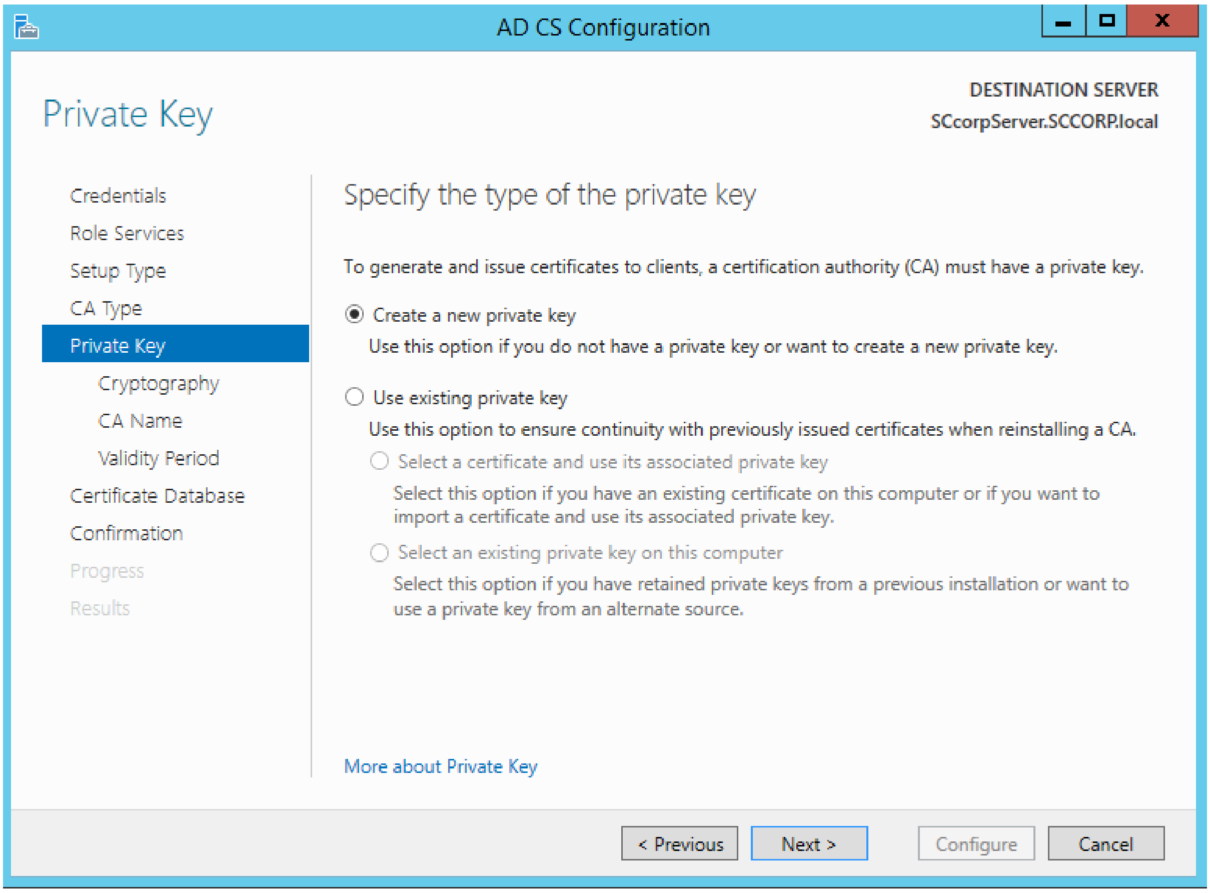
DESTINATION SERVER
SCcorpServer.SCCORP.local

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.



AD CS Configuration

Private Key

DESTINATION SERVER
SCcorpServer.SCCORP.local

Specify the type of the private key

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

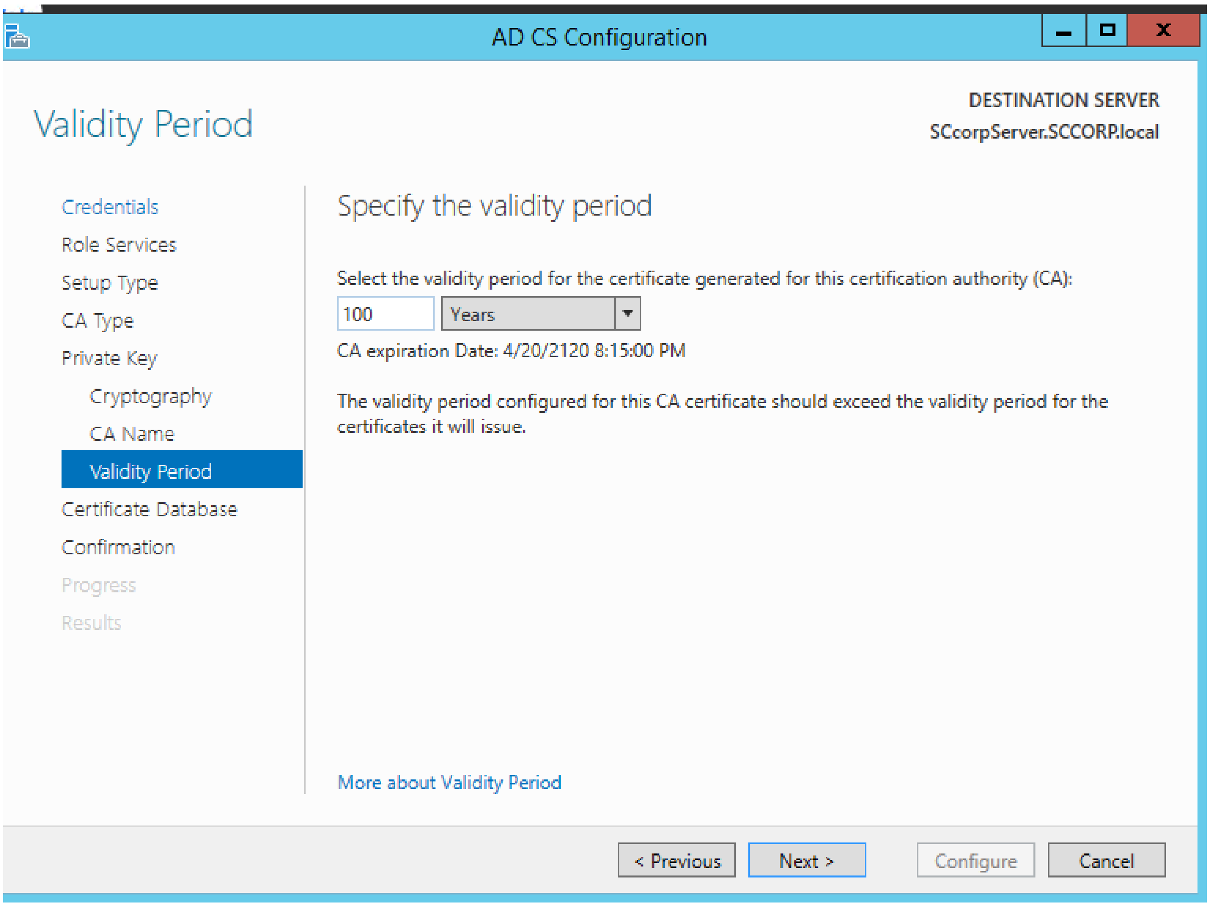
● Create a new private key
Use this option if you do not have a private key or want to create a new private key.

○ 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.

Set the validity period:



DESTINATION SERVER
SCcorpServer.SCCORP.local

Specify the validity period

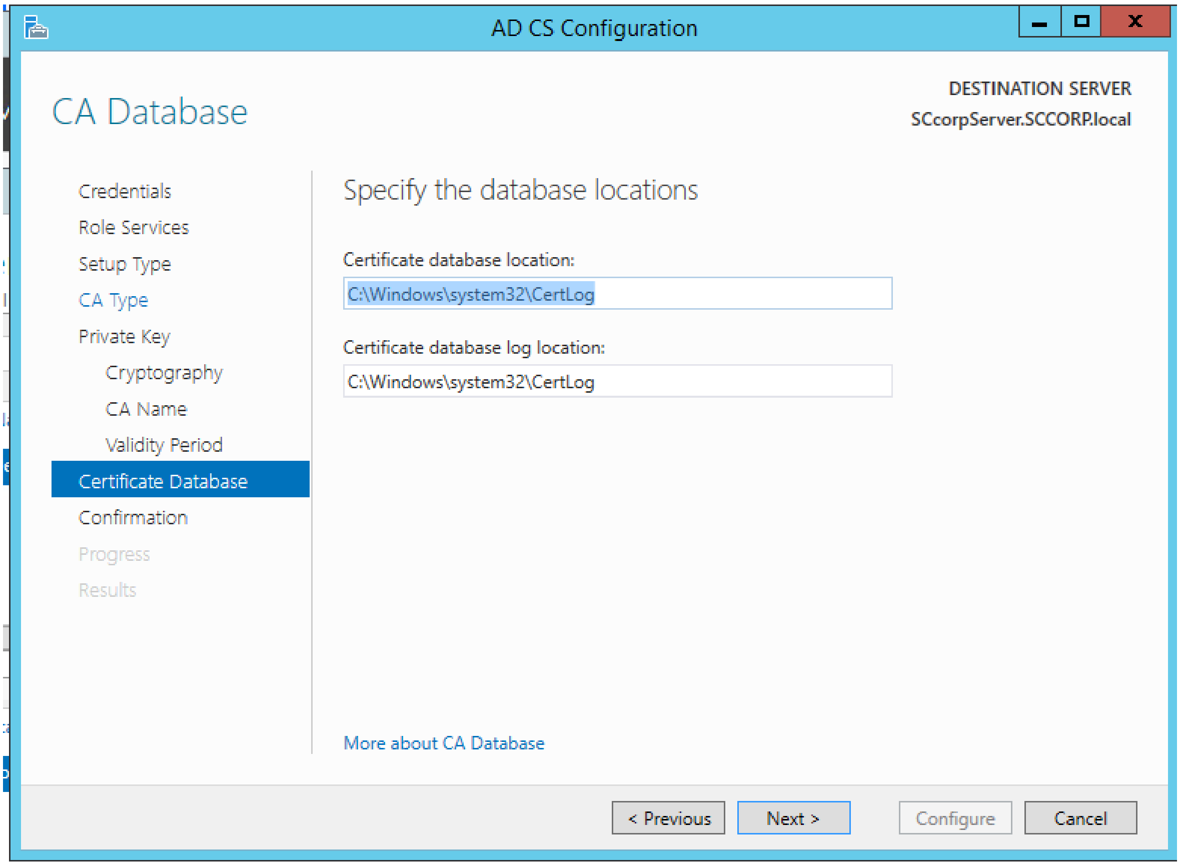
Select the validity period for the certificate generated for this certification authority (CA):

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.

Specify the database location:



DESTINATION SERVER
SCcorpServer.SCCORP.local

Specify the database locations

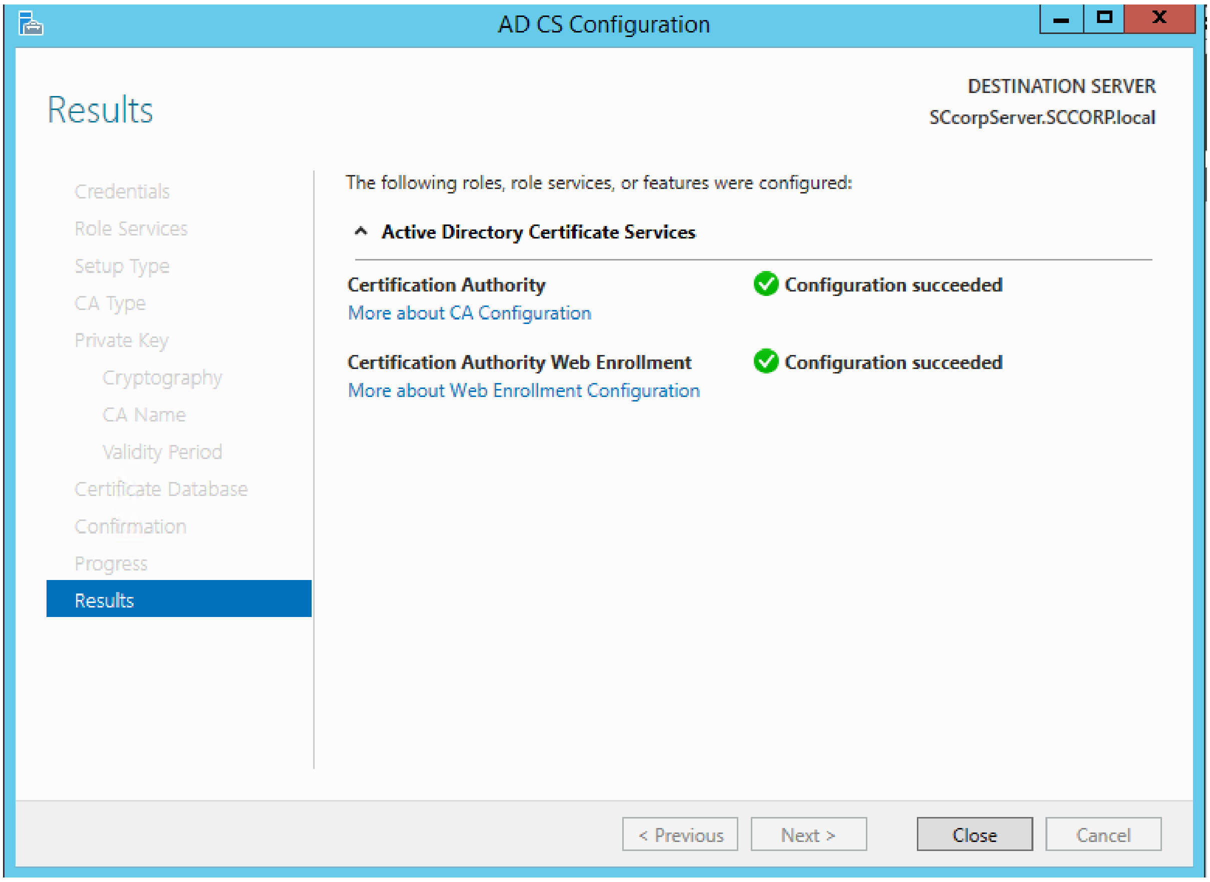
Certificate database location:

C:\Windows\system32\CertLog

Certificate database log location:

C:\Windows\system32\CertLog

Installation complete:



Results

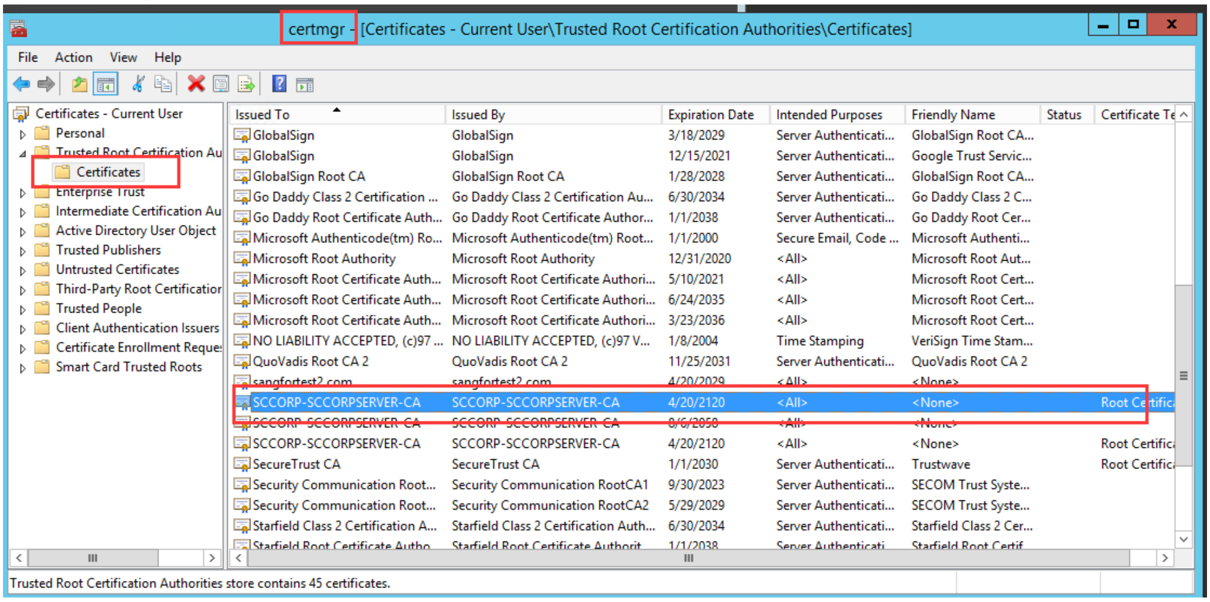
DESTINATION SERVER
SCcorpServer.SCCORP.local

The following roles, role services, or features were configured:

Active Directory Certificate Services

Certification Authority More about CA Configuration	✓ Configuration succeeded
Certification Authority Web Enrollment More about Web Enrollment Configuration	✓ Configuration succeeded

Go to certmgr.msc:

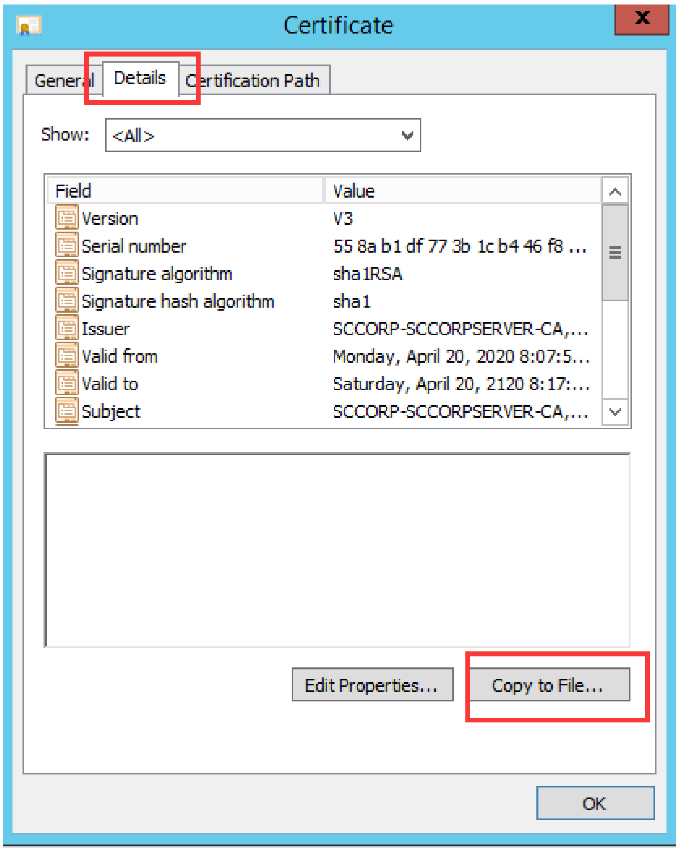

File
Action
View
Help
Certificates - Current User
Personal
Trusted Root Certification Au
Certificates
Enterprise Trust
Intermediate Certification Au
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification
Trusted People
Client Authentication Issuers
Certificate Enrollment Reque
Smart Card Trusted Roots

certmgr - [Certificates - Current User\Trusted Root Certification Authorities\Certificates]

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Te
GlobalSign	GlobalSign	3/18/2029	Server Authenticati...	GlobalSign Root CA...		
GlobalSign	GlobalSign	12/15/2021	Server Authenticati...	Google Trust Servic...		
GlobalSign Root CA	GlobalSign Root CA	1/28/2028	Server Authenticati...	GlobalSign Root CA...		
Go Daddy Class 2 Certification ...	Go Daddy Class 2 Certification Au...	6/30/2034	Server Authenticati...	Go Daddy Class 2 C...		
Go Daddy Root Certificate Auth...	Go Daddy Root Certificate Author...	1/1/2038	Server Authenticati...	Go Daddy Root Cer...		
Microsoft Authenticode(tm) Ro...	Microsoft Authenticode(tm) Root...	1/1/2000	Secure Email, Code ...	Microsoft Authenti...		
Microsoft Root Authority	Microsoft Root Authority	12/31/2020	<All>	Microsoft Root Aut...		
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	5/10/2021	<All>	Microsoft Root Cert...		
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	6/24/2035	<All>	Microsoft Root Cert...		
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	3/23/2036	<All>	Microsoft Root Cert...		
NO LIABILITY ACCEPTED, (c)97 ...	NO LIABILITY ACCEPTED, (c)97 V...	1/8/2004	Time Stamping	VeriSign Time Stam...		
QuoVadis Root CA 2	QuoVadis Root CA 2	11/25/2031	Server Authenticati...	QuoVadis Root CA 2		
sangfortest2.com	sangfortest2.com	4/20/2029	<All>	<None>		
SCCORP-SCCORPSERVER-CA	SCCORP-SCCORPSERVER-CA	4/20/2120	<All>	<None>		Root Certific
SCCORP-SCCORPSERVER-CA	SCCORP-SCCORPSERVER-CA	8/6/2050	<All>	<None>		
SCCORP-SCCORPSERVER-CA	SCCORP-SCCORPSERVER-CA	4/20/2120	<All>	<None>		Root Certific
SecureTrust CA	SecureTrust CA	1/1/2030	Server Authenticati...	Trustwave		Root Certific
Security Communication Root...	Security Communication RootCA1	9/30/2023	Server Authenticati...	SECOM Trust Syste...		
Security Communication Root...	Security Communication RootCA2	5/29/2029	Server Authenticati...	SECOM Trust Syste...		
Starfield Class 2 Certification A...	Starfield Class 2 Certification Auth...	6/30/2034	Server Authenticati...	Starfield Class 2 Cer...		
Starfield Root Certificate Autho...	Starfield Root Certificate Authorit...	1/1/2038	Server Authenticati...	Starfield Root Certif...		

Trusted Root Certification Authorities store contains 45 certificates.

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

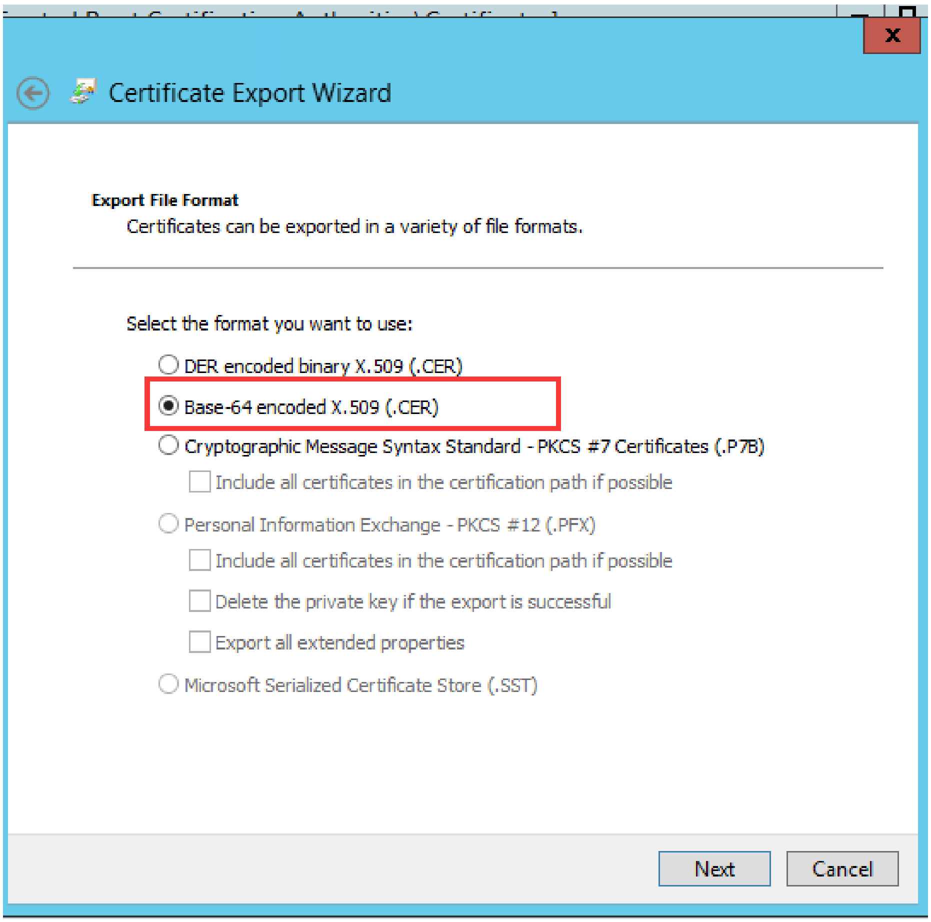


Certificate

General | Details | Certification Path

Show: <All>

Field	Value
Version	V3
Serial number	55 8a b1 df 77 3b 1c b4 46 f8 ...
Signature algorithm	sha1RSA
Signature hash algorithm	sha1
Issuer	SCCORP-SCCORPSERVER-CA,...
Valid from	Monday, April 20, 2020 8:07:5...
Valid to	Saturday, April 20, 2120 8:17:...
Subject	SCCORP-SCCORPSERVER-CA,...



Certificate Export Wizard

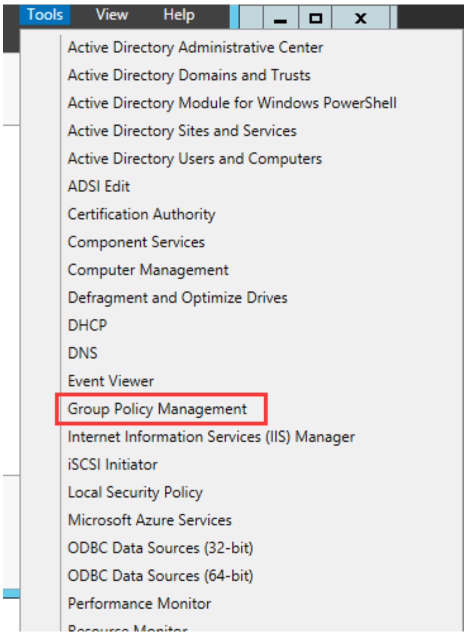
Export File Format
Certificates can be exported in a variety of file formats.

Select the format you want to use:

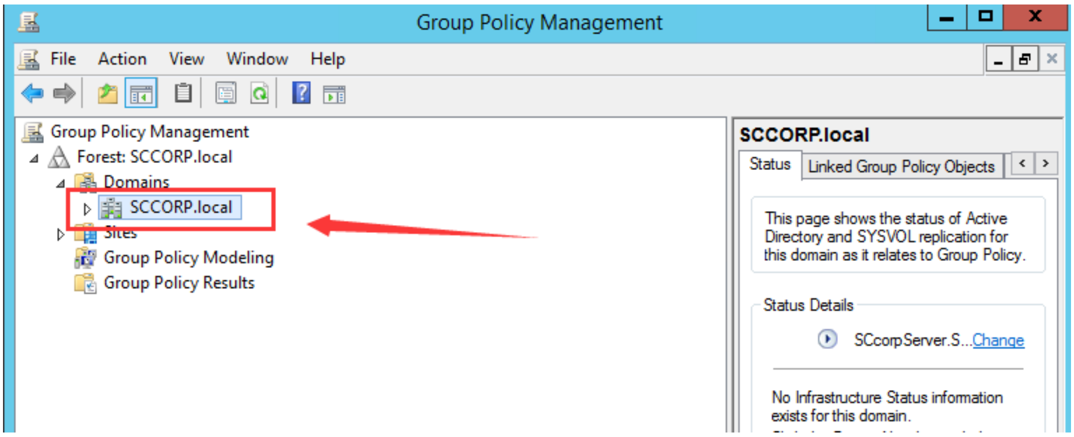
○ DER encoded binary X.509 (.CER)
● Base-64 encoded X.509 (.CER)
○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
□ Include all certificates in the certification path if possible
○ Personal Information Exchange - PKCS #12 (.PFX)
□ Include all certificates in the certification path if possible
□ Delete the private key if the export is successful
□ Export all extended properties
○ Microsoft Serialized Certificate Store (.SST)

4.3 Configuration of LDAPS Server Signing

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


Tools
View
Help
Active Directory Administrative Center
Active Directory Domains and Trusts
Active Directory Module for Windows PowerShell
Active Directory Sites and Services
Active Directory Users and Computers
ADSI Edit
Certification Authority
Component Services
Computer Management
Defragment and Optimize Drives
DHCP
DNS
Event Viewer
Group Policy Management
Internet Information Services (IIS) Manager
iSCSI Initiator
Local Security Policy
Microsoft Azure Services
ODBC Data Sources (32-bit)
ODBC Data Sources (64-bit)
Performance Monitor
Resource Monitor

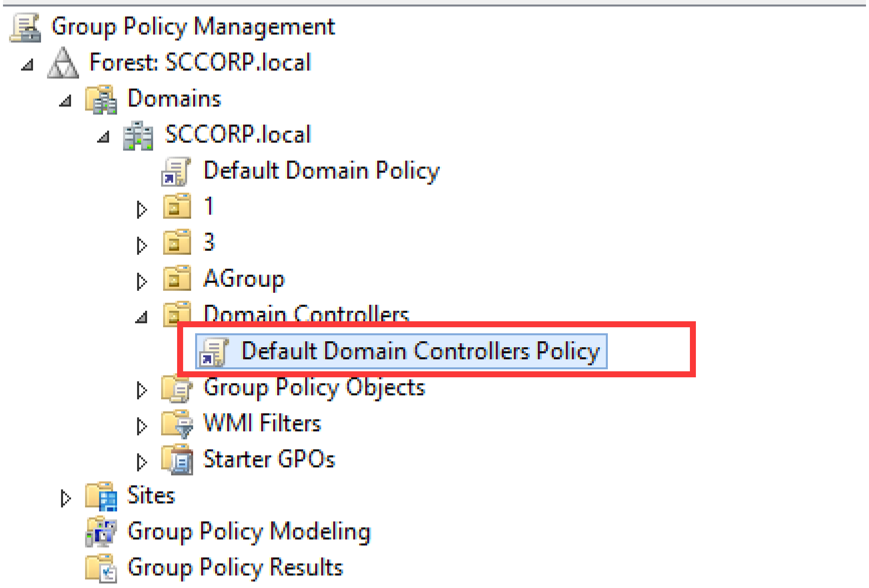
Choose the correct Domain name and Extend it.



This page shows the status of Active Directory and SYSVOL replication for this domain as it relates to Group Policy.

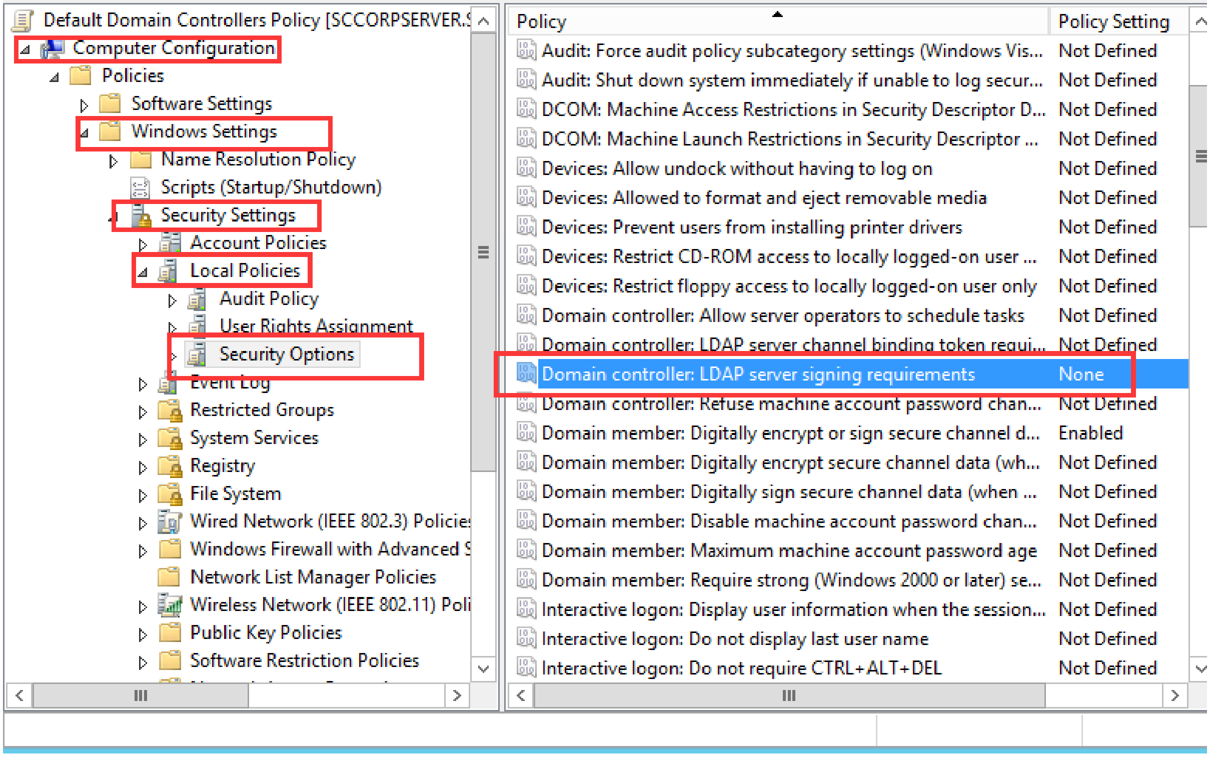
No Infrastructure Status information exists for this domain.

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



- Group Policy Management
  - Forest: SCCORP.local
    - Domains
      - SCCORP.local
        - Default Domain Policy
        - 1
        - 3
        - AGroup
        - Domain Controllers
          - Default Domain Controllers Policy
        - Group Policy Objects
        - WMI Filters
        - Starter GPOs
    - Sites
    - Group Policy Modeling
    - Group Policy Results

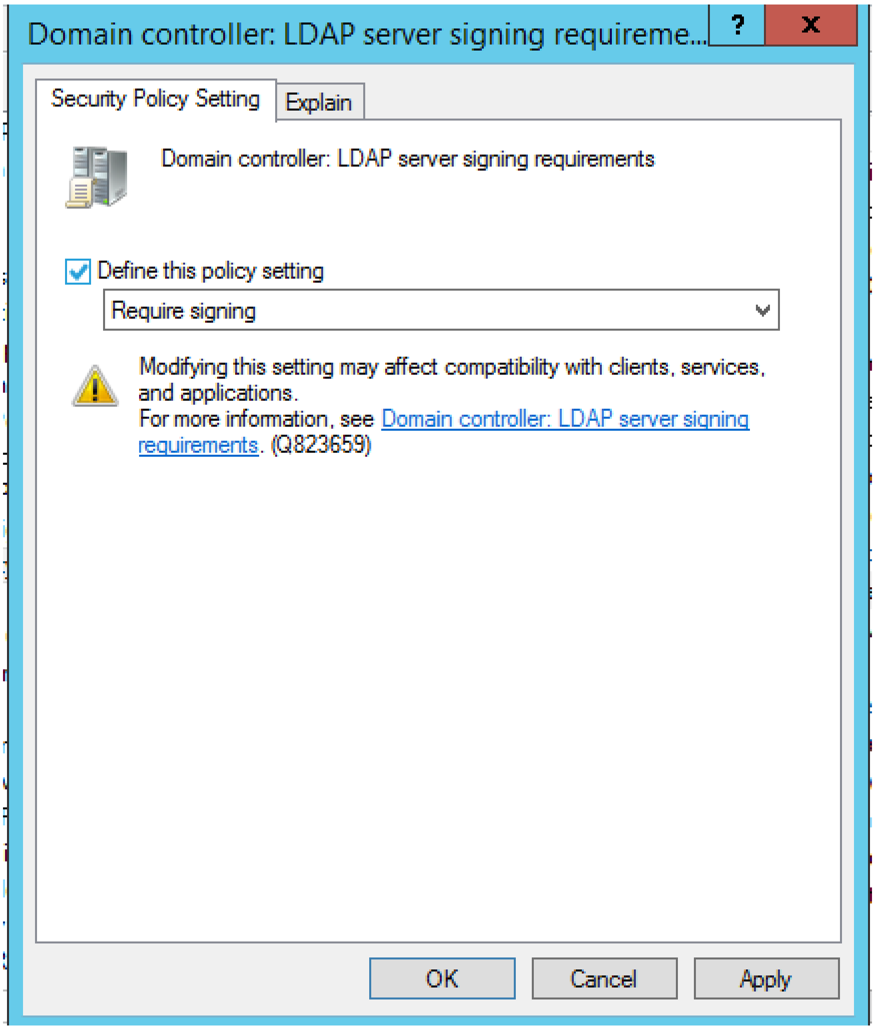
Right Click Edit and open the group management editor:



- Default Domain Controllers Policy [SCCORPSERVER.S
  - Computer Configuration
    - Policies
      - Software Settings
      - Windows Settings
        - Name Resolution Policy
        - Scripts (Startup/Shutdown)
        - Security Settings
          - Account Policies
          - Local Policies
            - Audit Policy
            - User Rights Assignment
            - Security Options
          - Event Log
          - Restricted Groups
          - System Services
          - Registry
          - File System
          - Wired Network (IEEE 802.3) Policie
          - Windows Firewall with Advanced S
          - Network List Manager Policies
          - Wireless Network (IEEE 802.11) Poli
          - Public Key Policies
          - Software Restriction Policies

Policy	Policy Setting
Audit: Force audit policy subcategory settings (Windows Vis...	Not Defined
Audit: Shut down system immediately if unable to log secur...	Not Defined
DCOM: Machine Access Restrictions in Security Descriptor D...	Not Defined
DCOM: Machine Launch Restrictions in Security Descriptor ...	Not Defined
Devices: Allow undock without having to log on	Not Defined
Devices: Allowed to format and eject removable media	Not Defined
Devices: Prevent users from installing printer drivers	Not Defined
Devices: Restrict CD-ROM access to locally logged-on user ...	Not Defined
Devices: Restrict floppy access to locally logged-on user only	Not Defined
Domain controller: Allow server operators to schedule tasks	Not Defined
Domain controller: LDAP server channel binding token requi...	Not Defined
Domain controller: LDAP server signing requirements	None
Domain controller: Refuse machine account password chan...	Not Defined
Domain member: Digitally encrypt or sign secure channel d...	Enabled
Domain member: Digitally encrypt secure channel data (wh...	Not Defined
Domain member: Digitally sign secure channel data (when ...	Not Defined
Domain member: Disable machine account password chan...	Not Defined
Domain member: Maximum machine account password age	Not Defined
Domain member: Require strong (Windows 2000 or later) se...	Not Defined
Interactive logon: Display user information when the session...	Not Defined
Interactive logon: Do not display last user name	Not Defined
Interactive logon: Do not require CTRL+ALT+DEL	Not Defined

Change the setting to Required signing.



Domain controller: LDAP server signing requireme...

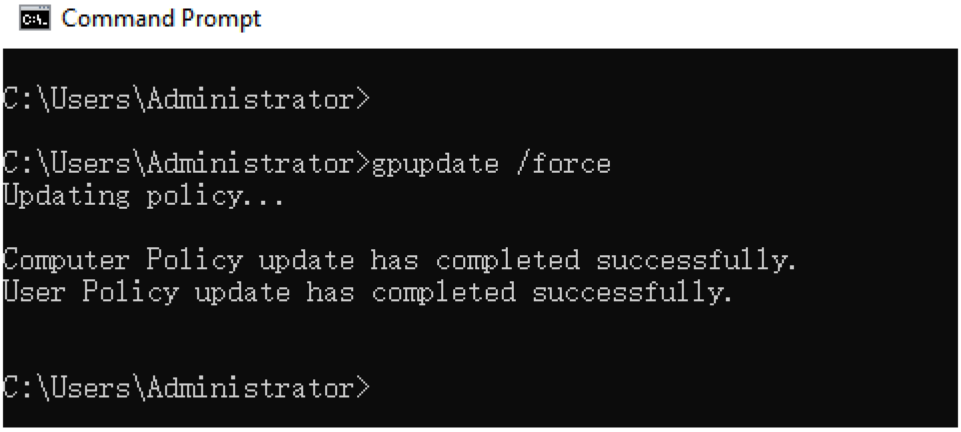
Domain controller: LDAP server signing requirements

☑ Define this policy setting

Require signing

Modifying this setting may affect compatibility with clients, services, and applications.
For more information, see Domain controller: LDAP server signing requirements. (Q823659)

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



```
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>
```

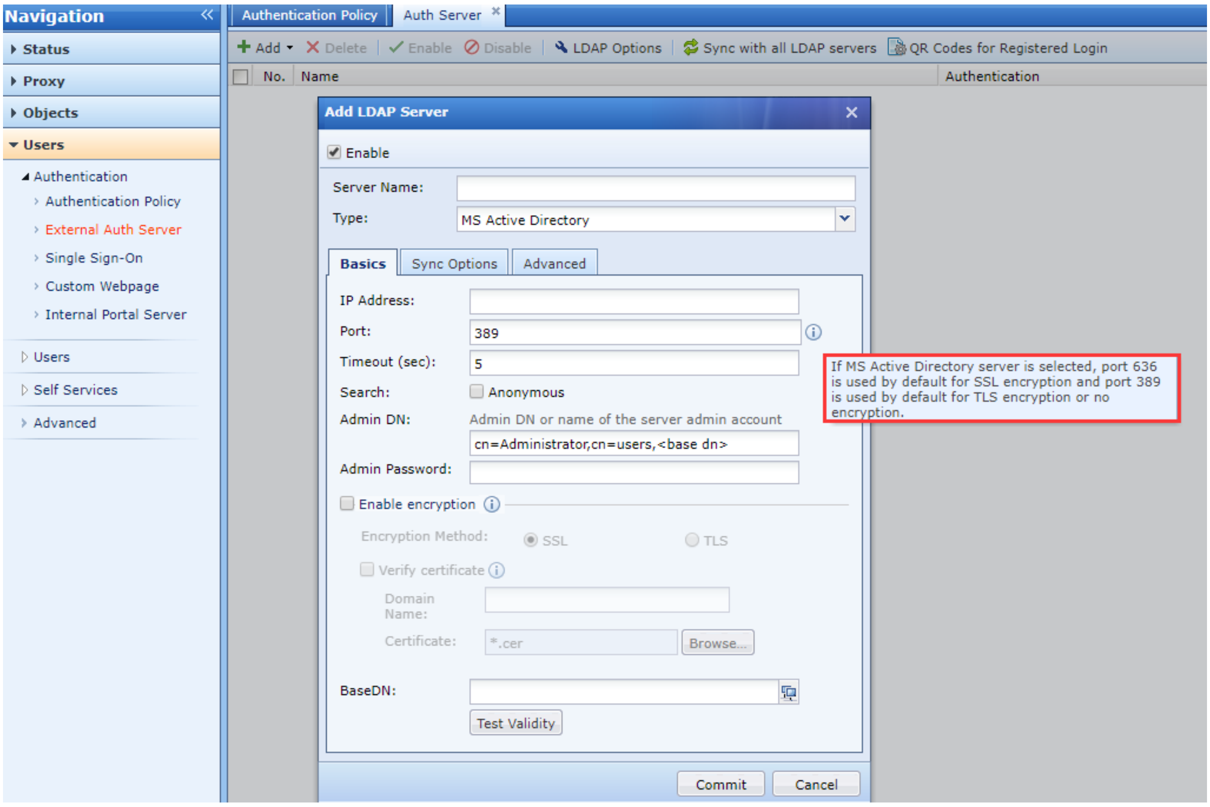
4.4 AD Configuration on IAM

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

4.4.1 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.



☑ Enable

Server Name:

Type: MS Active Directory

IP Address:

Port: 389

Timeout (sec): 5

Search: □ Anonymous

Admin DN: Admin DN or name of the server admin account

cn=Administrator,cn=users,<base dn>

Admin Password:

□ Enable encryption

Encryption Method: ● SSL ○ TLS

□ Verify certificate

Domain Name:

Certificate: *.cer

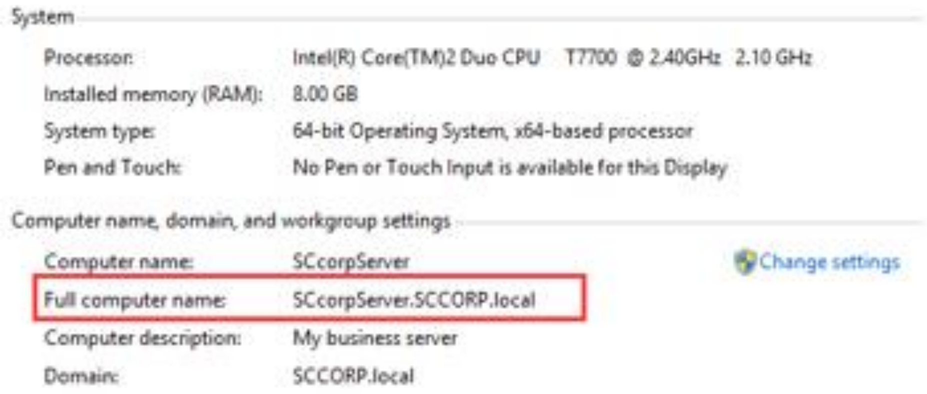
BaseDN:

If MS Active Directory server is selected, port 636 is used by default for SSL encryption and port 389 is used by default for TLS encryption or no encryption.

4.4.2 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:



System

Processor: Intel(R) Core(TM)2 Duo CPU T7700 @ 2.40GHz 2.10 GHz

Installed memory (RAM): 8.00 GB

System type: 64-bit Operating System, x64-based processor

Pen and Touch: No Pen or Touch Input is available for this Display

Computer name, domain, and workgroup settings

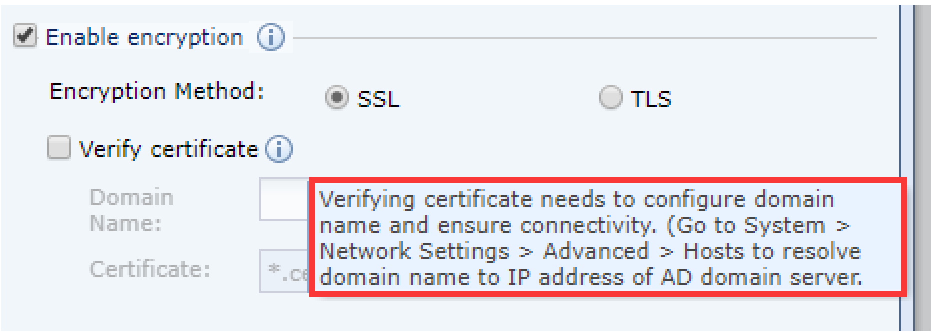
Computer name: SCcorpServer

Full computer name: SCcorpServer.SCCORP.local

Computer description: My business server

Domain: SCCORP.local

- 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:



☑ Enable encryption

Encryption Method: ● SSL ○ TLS

□ Verify certificate

Domain Name:

Certificate: *.ce

Verifying certificate needs to configure domain name and ensure connectivity. (Go to System > Network Settings > Advanced > Hosts to resolve domain name to IP address of 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.

SANGFOR

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