Authentication of Fabric OS users using LDAP

This document describes the steps involved in configuring the Active Directory infrastructure, the account information and the Fabric OS configuration in order to successfully authenticate against accounts stored in an Active Directory based LDAP.

This in no official Brocade documentation. No warranties or liabilities given. Please refer to the Fabric OS Administrators Guide for official documentation.

FOS Authentication using LDAP

Fabric OS v6.0.0 and later supports the use of both the local user database and lightweight directory access protocol (LDAP) using Microsoft Active Directory in Windows at the same time.

When configured to use LDAP, the switch acts as a network access server (NAS) and LDAP client. The switch sends all authentication, authorization, and accounting (AAA) service requests to the LDAP server. The LDAP server receives the request, validates the request, and sends its response back to the switch. The supported management access channels that integrate with LDAP include serial port, Telnet, SSH, Web Tools, and API. A switch can be configured to try both LDAP and local switch authentication.

When configured for LDAP, a switch becomes a LDAP client. Authentication records are stored in the LDAP host server database. Login and logout account name, assigned role, and time-accounting records are also stored on the LDAP server for each user. By default, the LDAP services are disabled, so AAA services default to the switch local database.

Multiple login sessions can configure simultaneously, and the last session to apply a change leaves its configuration in effect. After a configuration is applied, it persists after a reboot or an HA failover.

The configuration applies to all switches and on a director the configuration replicates itself on a standby CP blade if one is present. It is saved in a configuration upload and applied in a configuration download. You should configure at least two LDAP servers so that if one fails, the other will assume service. You can set the configuration with both LDAP

service and local authentication enabled so that if the LDAP servers do not respond due to power failure or network problems, the switch uses local authentication.

Consider the following effects of the use of LDAP service on other Fabric OS features:

When LDAP service is enabled, all account passwords must be managed on the LDAP server. The Fabric OS mechanisms for changing switch passwords remain functional; however, such changes affect only the involved switches locally. They do not propagate to the LDAP server, nor do they affect any account on the LDAP server. When LDAP is set up for a fabric that contains a mix of switches with and without LDAP support, the way a switch authenticates users depends on whether a LDAP server is set up for that switch. For a switch with LDAP support and configuration, authentication bypasses the local password database. For a switch without LDAP support or configuration, authentication uses the switch's local account names and passwords.

The following behaviors apply to Web Tools:

- Web Tools client and server keep a session open after a user is authenticated. A password change on a switch invalidates an open session and requires the user to log in again. When integrated with LDAP, a switch password change on the LDAP server does not invalidate an existing open session, although a password change on the local switch does.
- If you cannot log in because of a LDAP server connection problem, Web Tools displays a message indicating server outage

LDAP configuration and Microsoft Active Directory

LDAP provides user authentication and authorization using the Microsoft Active Directory service in conjunction with a LDAP client on the switch. There are two modes of operation in LDAP authentication, FIPS mode and non-FIPS mode. This section discusses LDAP authentication in non-FIPS mode.

The following restrictions apply when using LDAP:

- There is no password change through Active Directory.
- There is no automatic migration of newly created users from the local switch database to Active Directory.
- Only IPv4 is supported for LDAP on Windows 2000 and LDAP on Windows Server 2003.
- For LDAP on Windows Server 2008, both IPv4 and IPv6 are supported.
- LDAP authentication is used on the local switch only and not for the entire fabric.
- You can use the User-Principal-Name and not the Common-Name for AD LDAP authentication.
- To provide backward compatibility, authentication based on the Common Name is still supported for Active Directory LDAP 2000 and 2003. Common Name-based authentication is not recommended for new installations.
- A user can belong to multiple groups as long as one of the groups is the primary group. The primary group in the AD server should not be set to the group corresponding to the switch role. You can choose any other group.
- A user can be part of any Organizational Unit (OU).
- Active Directory LDAP 2000, 2003, and 2008 are supportedTo enable the secure LDAP service, you must install a certificate from the Microsoft Active Directory server or the OpenLDAP server. By default, the LDAP service does not require certificates.

When authentication is performed by User-Principal-Name, in Fabric OS 7.1.0 and later releases, the suffix part of the name (the @domain-name part) can be omitted when the user logs in. If the suffix part of the User-Principal-Name name is omitted, the domain name configured for the LDAP server (in the aaaConfig --add server -d domain command) is added and used for authentication purposes.

Roles for Brocade-specific users can be added through the Microsoft Management Console.

Groups created in Active Directory must correspond directly to the RBAC user roles on the switch. Role assignments can be achieved by including the user in the respective group. A user can be assigned to multiple groups such as Switch Admin and Security Admin. For LDAP servers, you can use the ldapCfg --maprole ldap_role_name switch_role command to map LDAP server permissions to one of the default roles available on a switch

Brocade recommends configuring at least two authentication servers, so that if one fails, the other will assume service. Up to five servers are supported. Also the Switch local database should be configured as a backup and the passwords of the local users been unknown to anyone and stored safely.

The following is an overview of the process used to set up LDAP:

1. If your Windows Active Directory server for LDAP needs to be verified by the LDAP client (that is, the Brocade switch), then you must install a Certificate Authority (CA) certificate on the Windows Active Directory server for LDAP.
   Follow Microsoft instructions for generating and installing CA certificates on a Windows server.
2. Create a user in Microsoft Active Directory server. For instructions on how to create a user, refer to www.microsoft.com or Microsoft documentation to create a user in your Active Directory.
3. Create a group name that uses the switch's role name so that the Active Directory group's name is the same as the switch's role name.
   or
   Use the ldapCfg --maprole ldap_role_name switch_role command to map an LDAP server role to one of the default roles available on the switch.
4. Associate the user to the group by adding the user to the group.
5. Add the user's Administrative Domains or Virtual Fabrics to the CN_list by either editing the adminDescription value or adding the brcdAdVfData attribute to the existing Active Directory schema.

   This action maps the Admin Domains or Virtual Fabrics to the user name. Multiple Admin Domains can be added as a string value separated by the underscore character (_). Virtual Fabrics are added as a string value separate by a comma (,) and entered as a range.

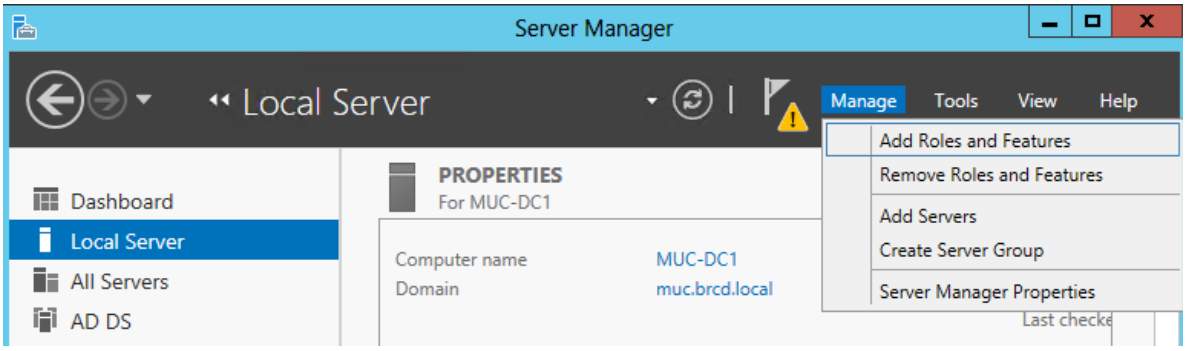
Install a Certificate authority (CA)

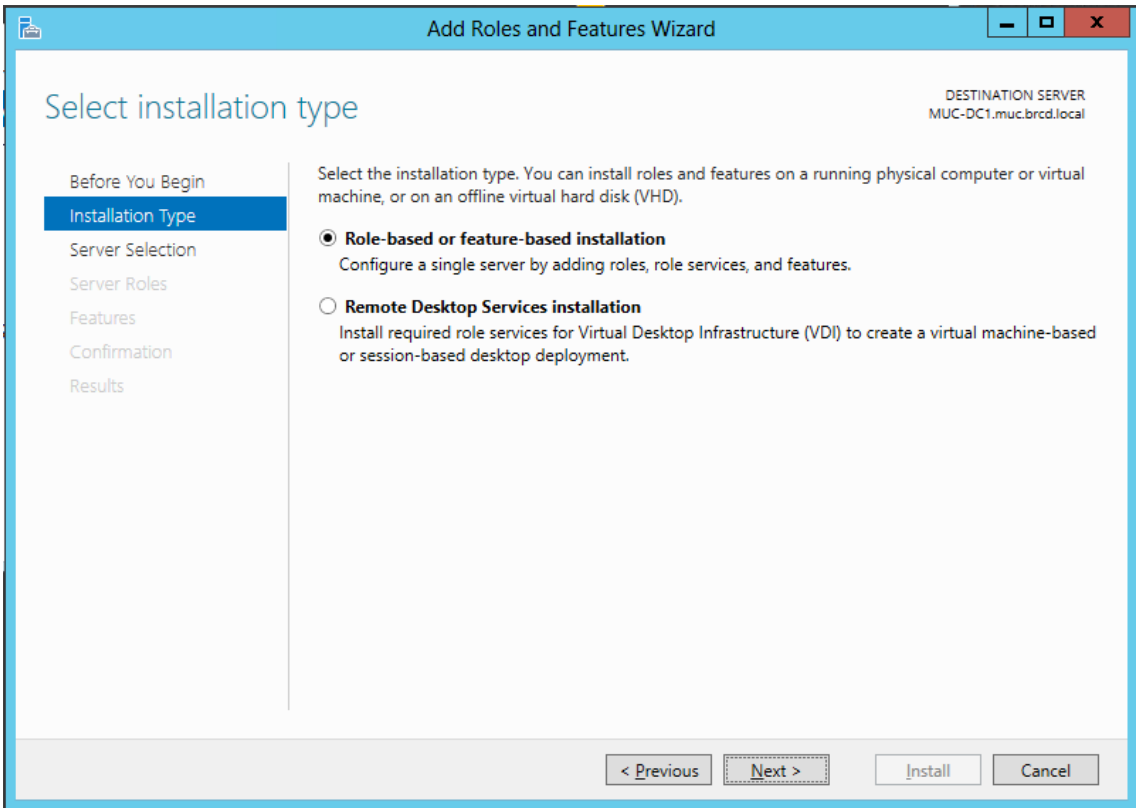
All communication using the LDAP protocol is clear text. As the communication between Fabric OS and the Microsoft Active Directory involves User IDs and Passwords TLS according to RFC 2246 is being used to encrypt the communication between Fabric OS and the Active Directory LDAP server.

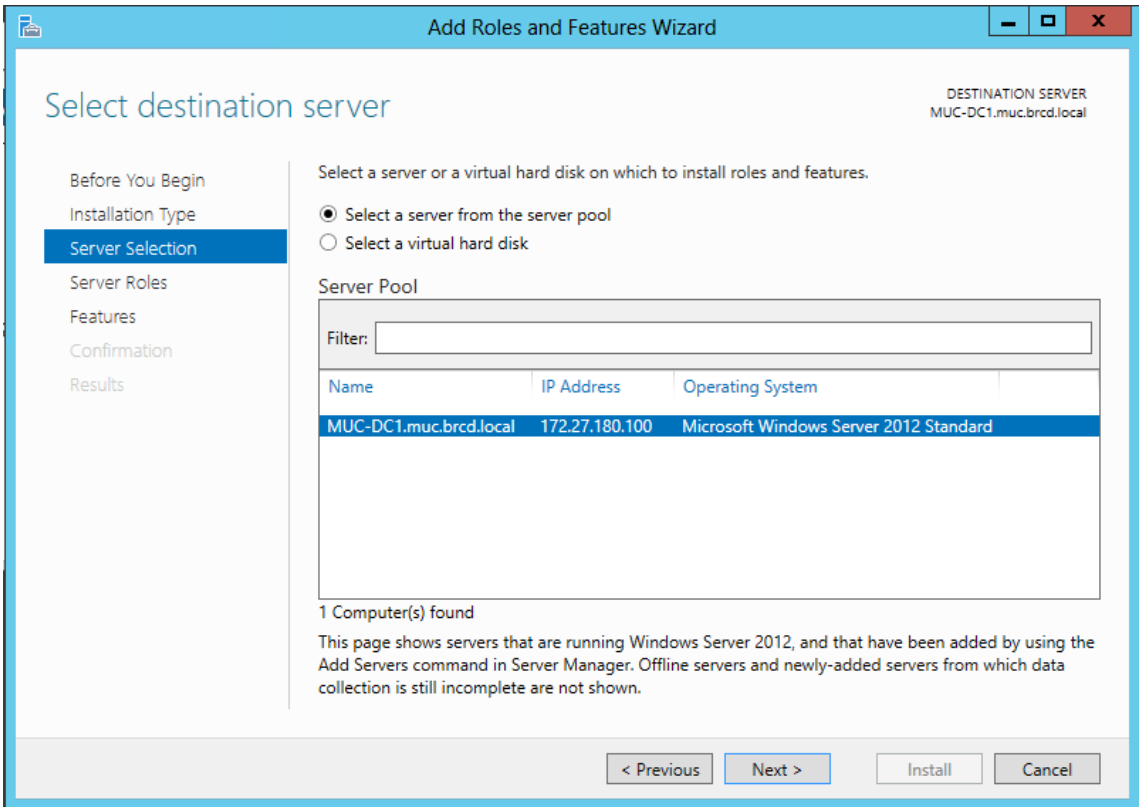
For authentication purposes, the Handshake Protocol uses an X.509 certificate to provide strong evidence to a second party that helps prove the identity of the party that holds the certificate and the corresponding private key. A certificate is a digital form of identification that is usually issued by a certification authority (CA) and contains identification information, a validity period, a public key, a serial number, and the digital signature of the issuer.

For TLS to work a CA has to be installed on a Member Server or Domain Controller of the Active Directory Domain:

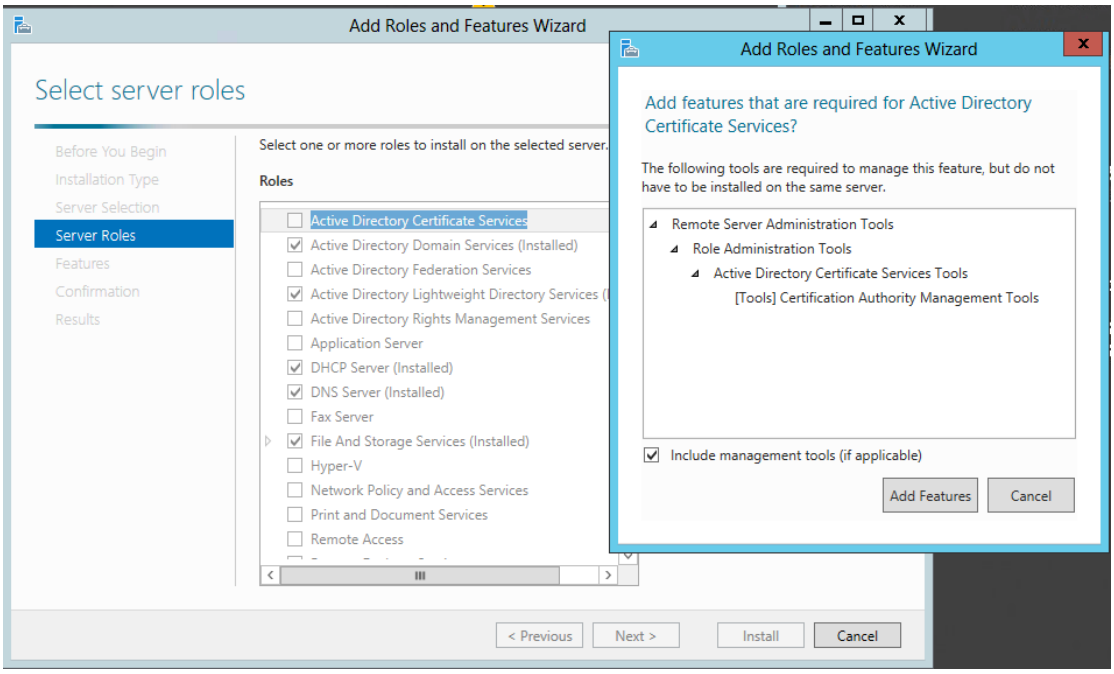
Start Server Manager and "Add Roles and Features" Dialog:

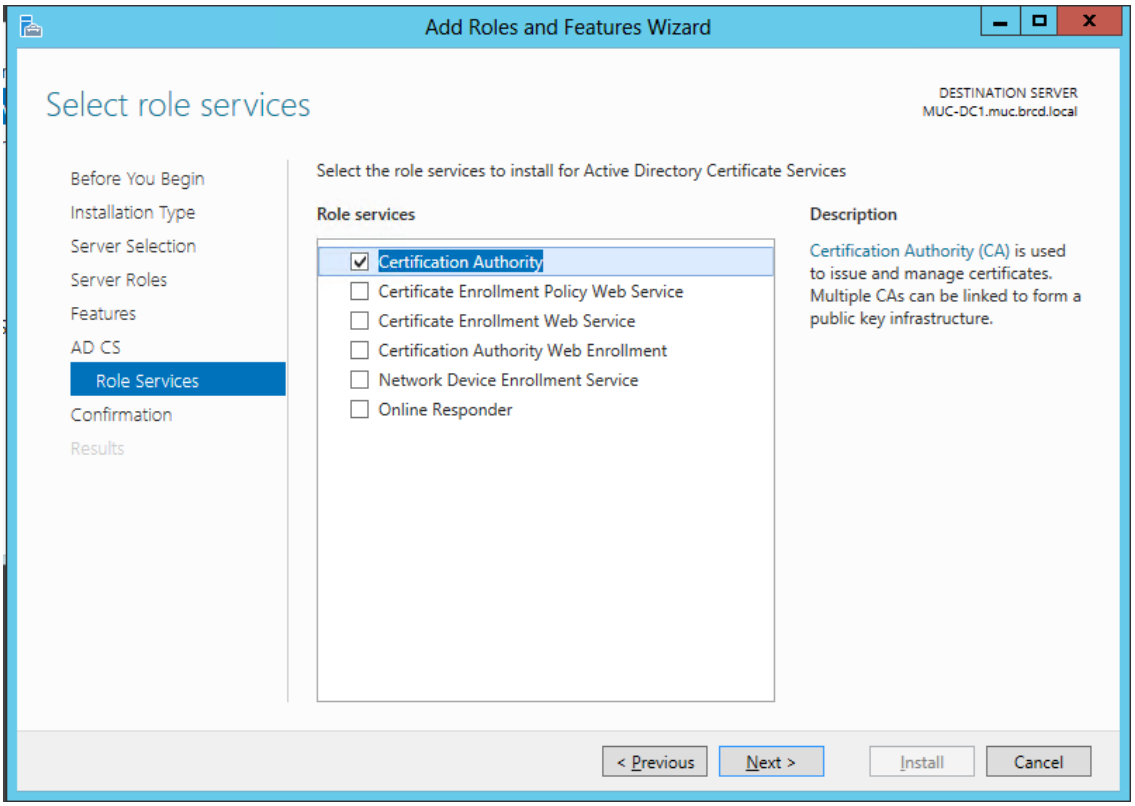


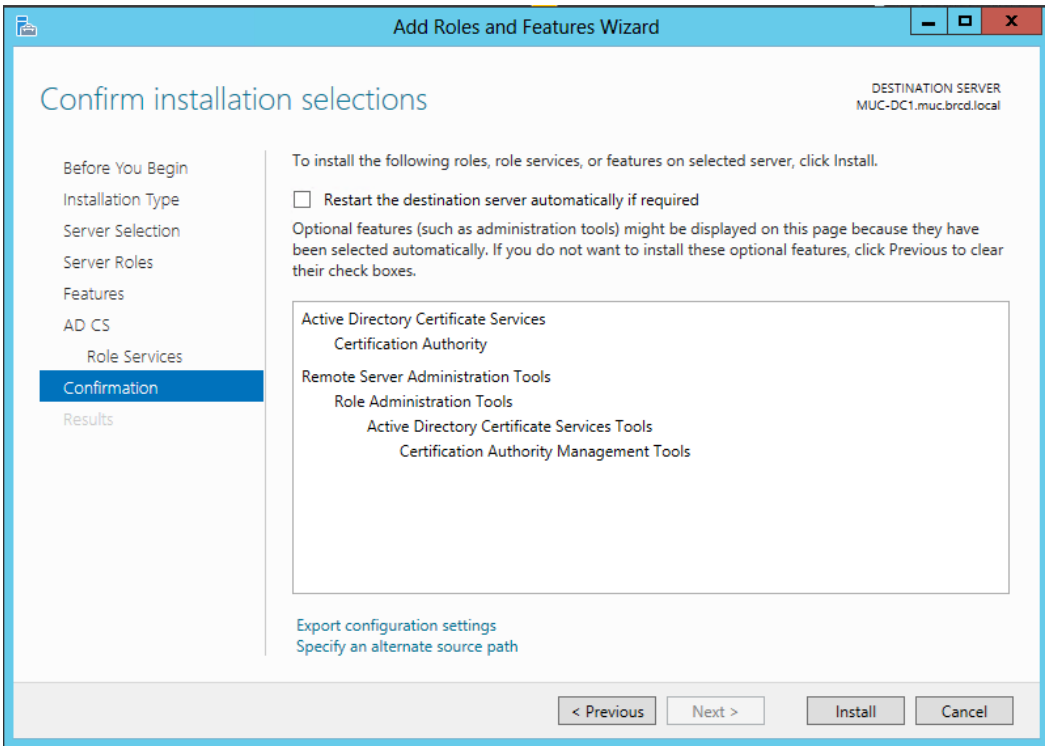

Add Roles and Features Wizard
Select installation type
DESTINATION SERVER
MUC-DC1.muc.brcd.local
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).
Role-based or feature-based installation
Configure a single server by adding roles, role services, and features.
Remote Desktop Services installation
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.
< Previous
Next >
Install
Cancel


Add Roles and Features Wizard
Select destination server
DESTINATION SERVER
MUC-DC1.muc.brcd.local
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select a server or a virtual hard disk on which to install roles and features.
Select a server from the server pool
Select a virtual hard disk
Server Pool
Filter:
Name
IP Address
Operating System
MUC-DC1.muc.brcd.local
172.27.180.100
Microsoft Windows Server 2012 Standard
1 Computer(s) found
This page shows servers that are running Windows Server 2012, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.
< Previous
Next >
Install
Cancel

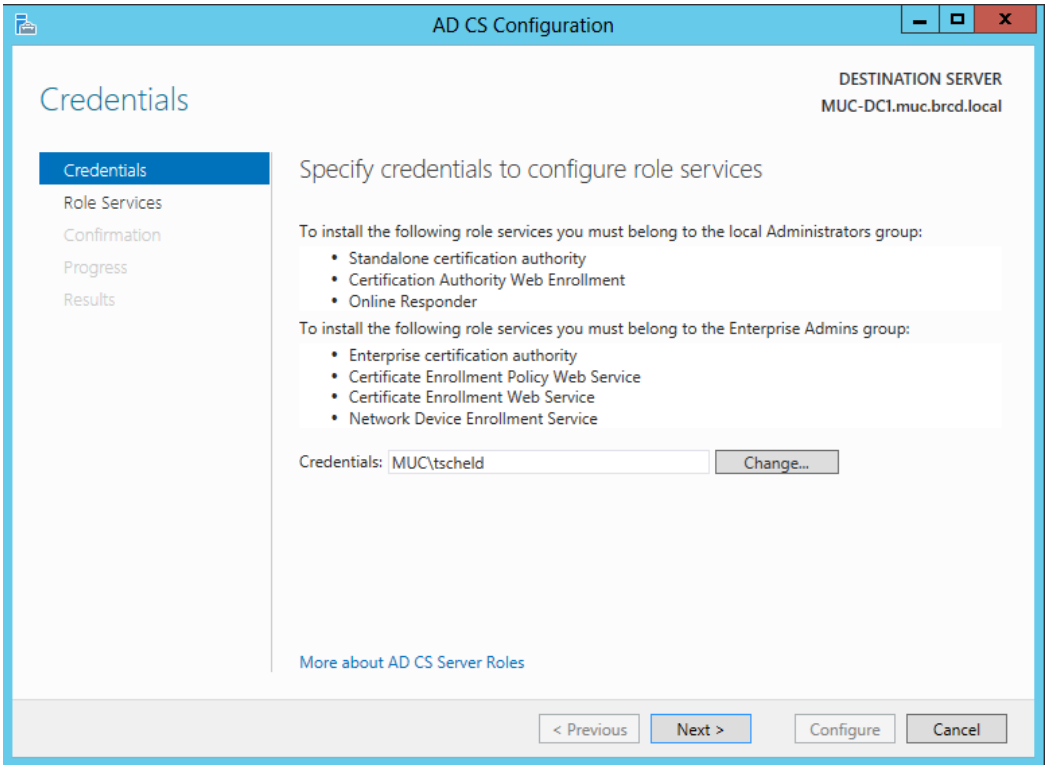
Check Active Directory Certificate Service.

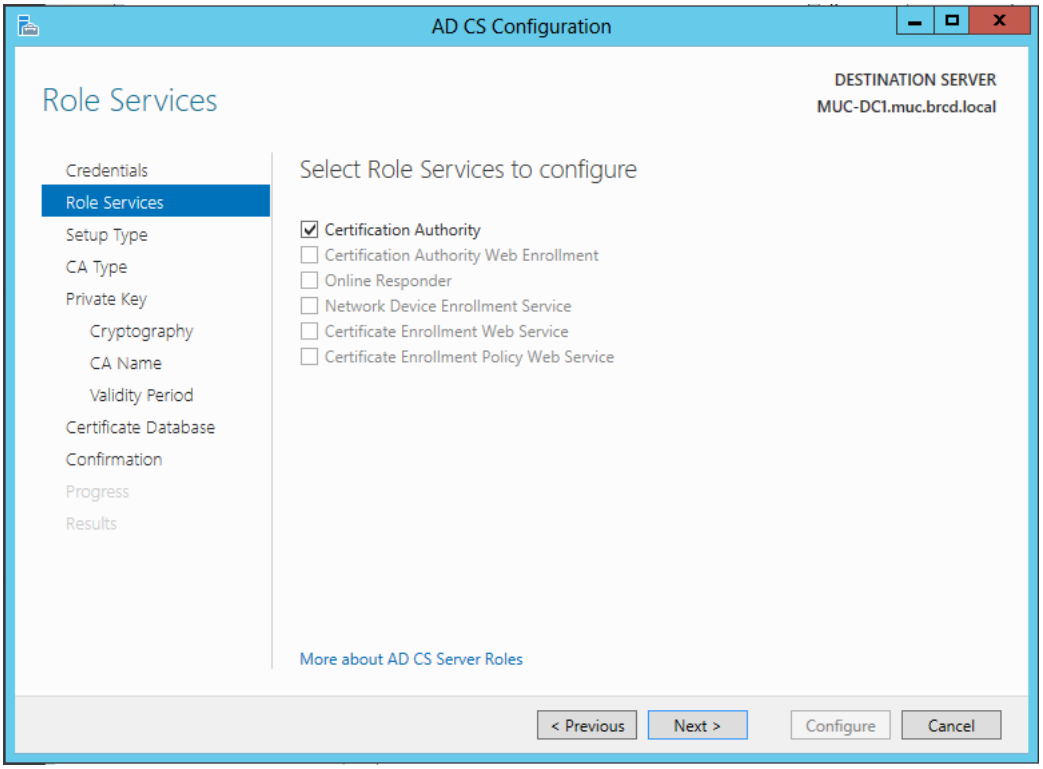


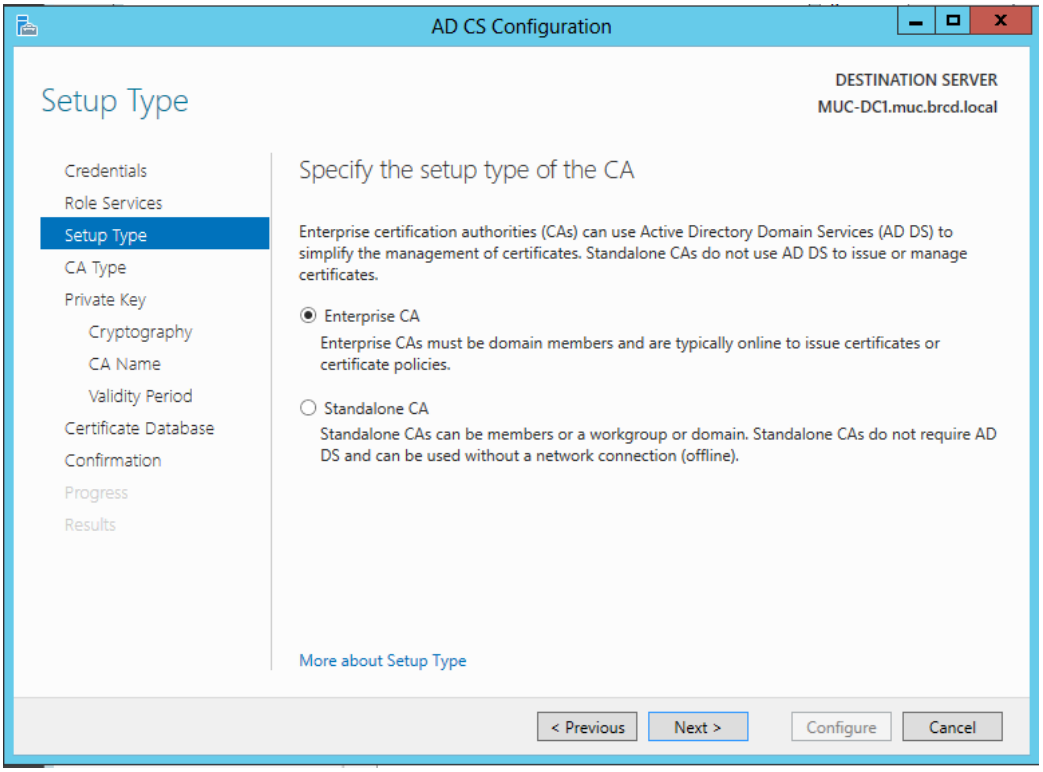


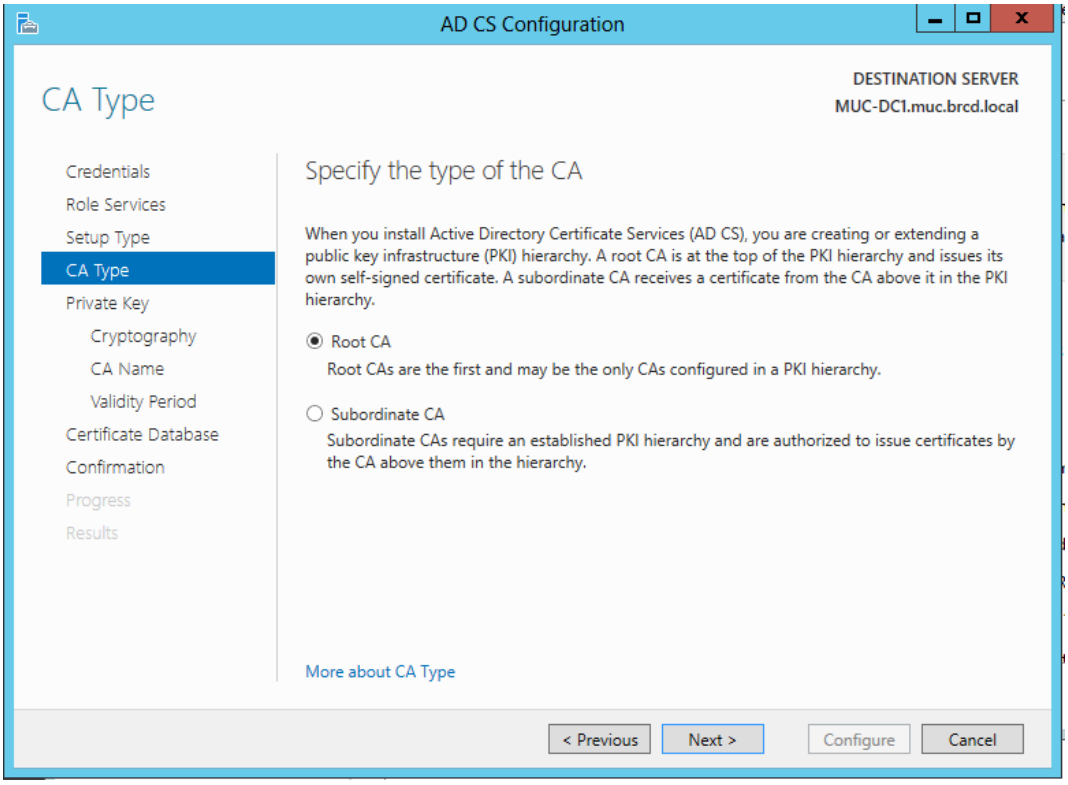


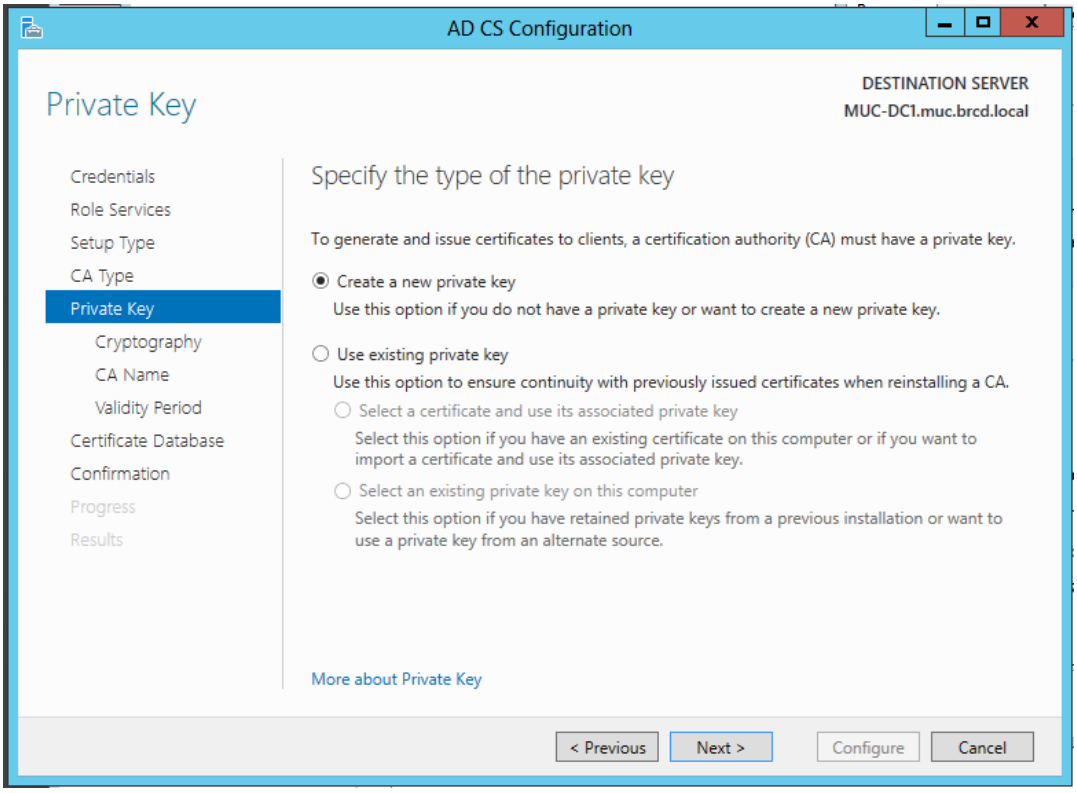
Start AD CS Configuration

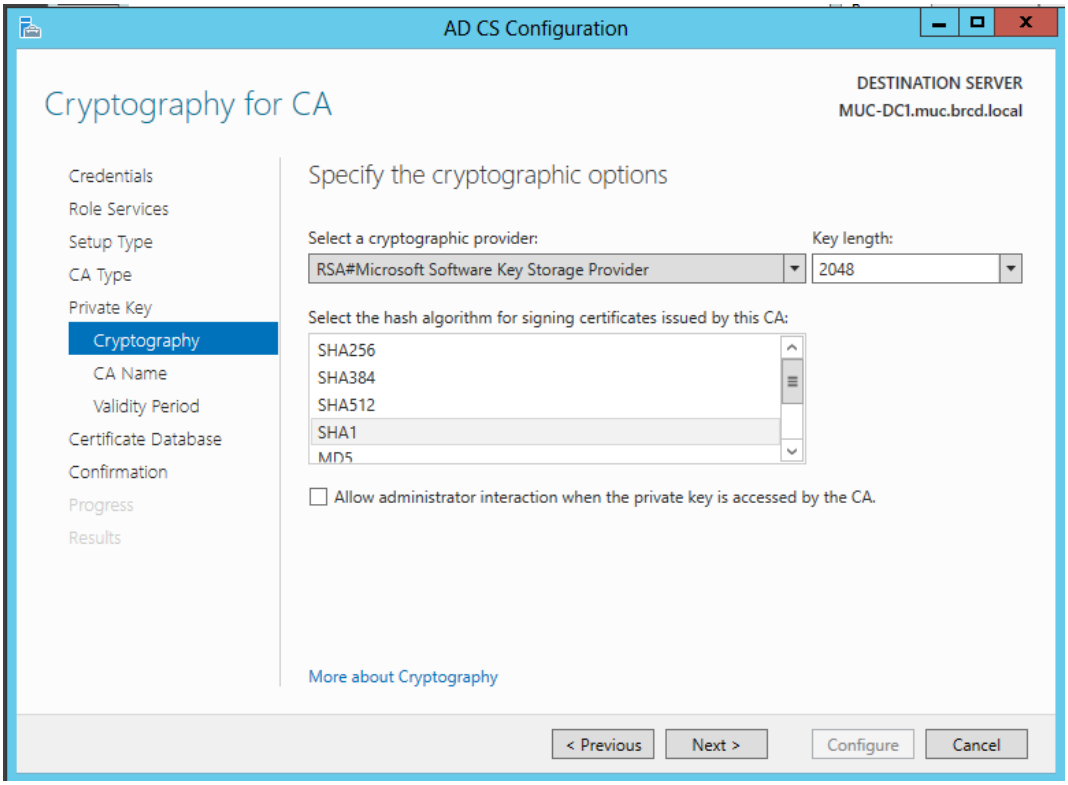


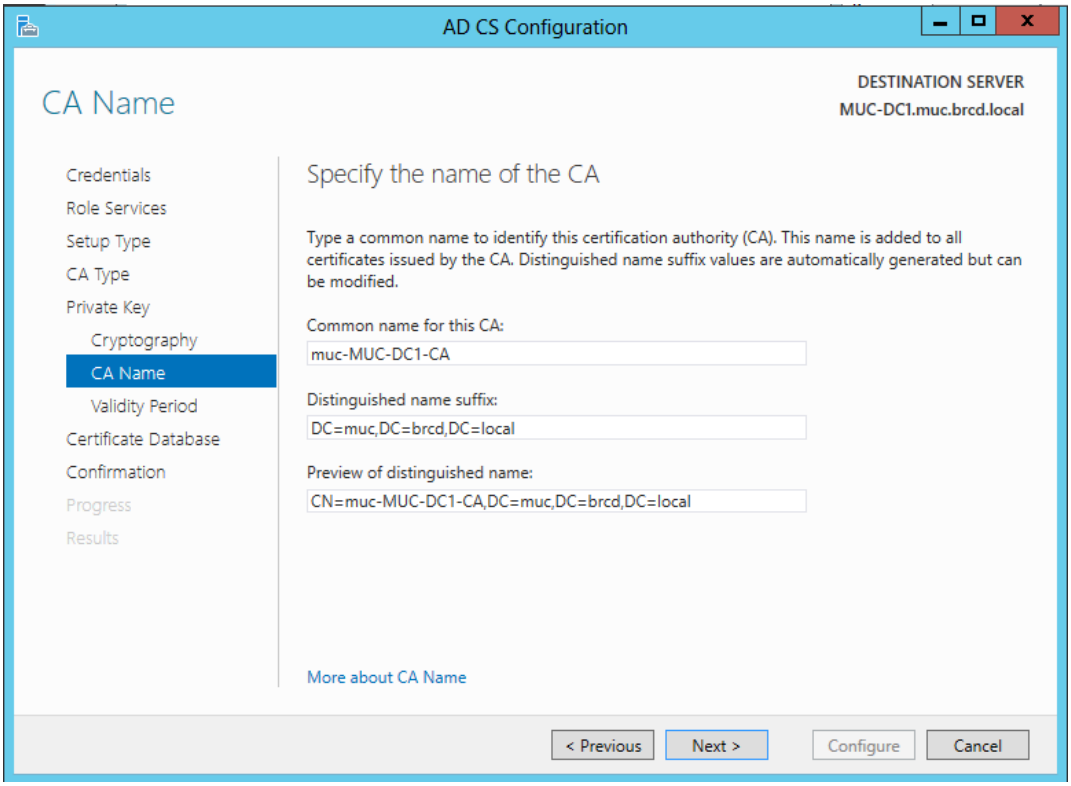

AD CS Configuration
Role Services
DESTINATION SERVER
MUC-DC1.muc.brcd.local
Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results
Select Role Services to configure
Certification Authority
Certification Authority 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

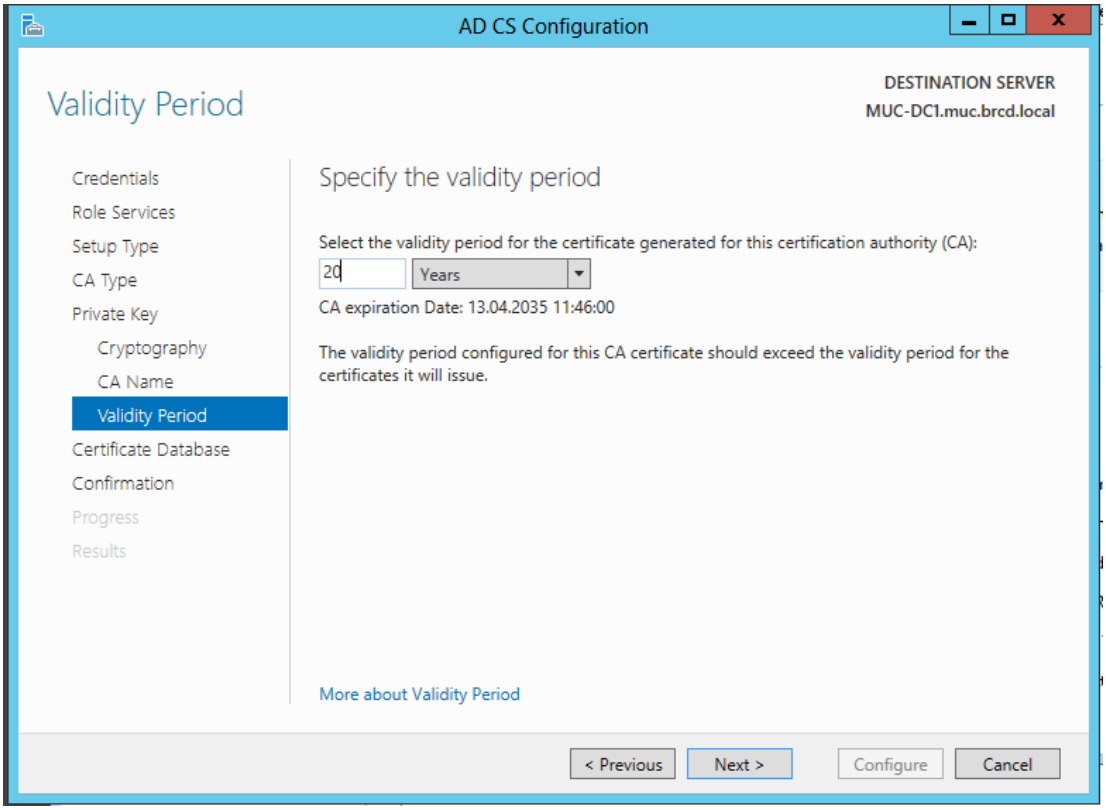

AD CS Configuration
Setup Type
DESTINATION SERVER
MUC-DC1.muc.brcd.local
Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results
Specify the setup type of the CA
Enterprise certification authorities (CAs) can use 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).
More about Setup Type
< Previous
Next >
Configure
Cancel

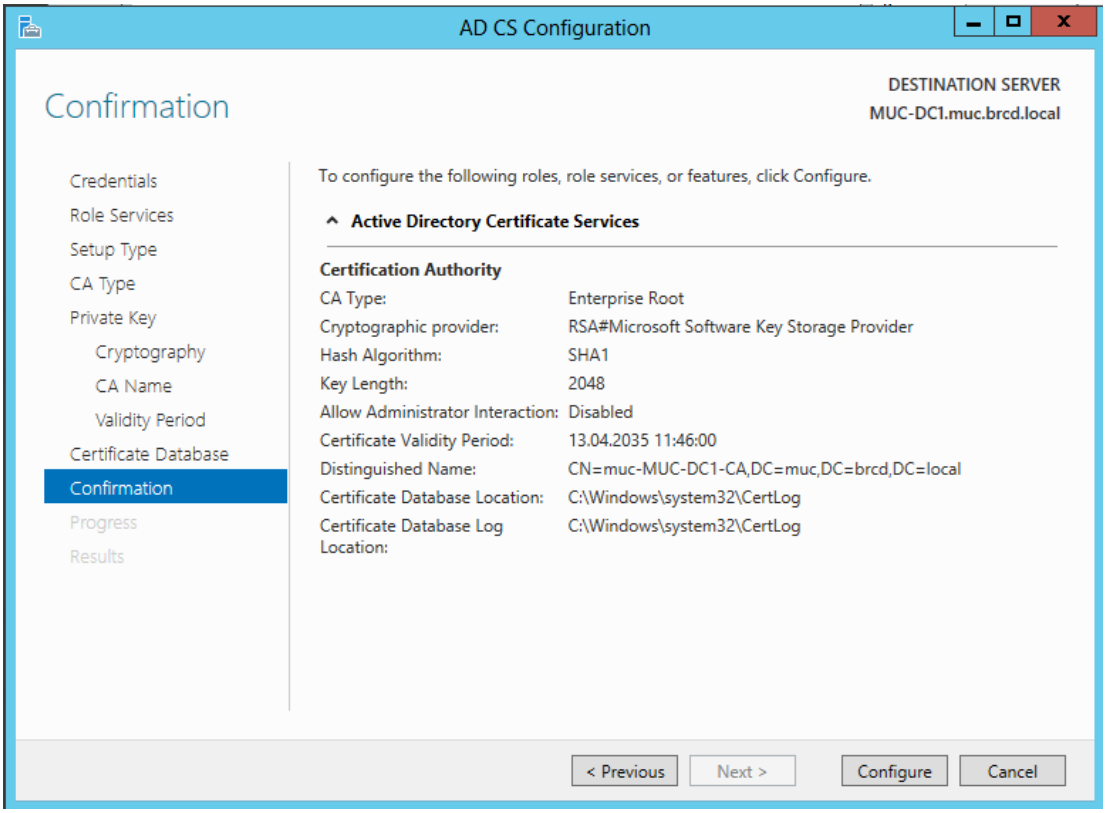

AD CS Configuration
CA Type
DESTINATION SERVER
MUC-DC1.muc.brcd.local
Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results
Specify the type of the CA
When you install Active Directory Certificate Services (AD 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

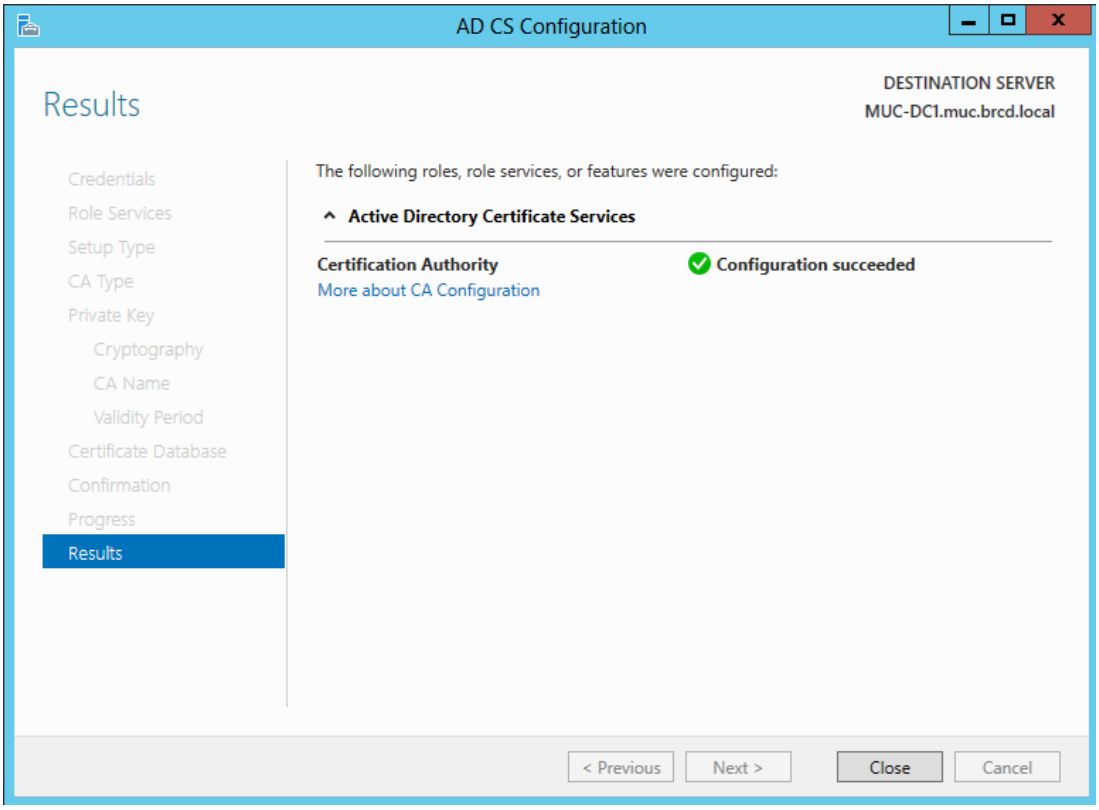

AD CS Configuration
Private Key
DESTINATION SERVER
MUC-DC1.muc.brcd.local
Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results
Specify the type of the private key
To generate and issue certificates to clients, 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


AD CS Configuration
Cryptography for CA
DESTINATION SERVER
MUC-DC1.muc.brcd.local
Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results
Specify the cryptographic options
Select a cryptographic provider:
RSA#Microsoft Software Key Storage Provider
Key length:
2048
Select the hash algorithm for signing certificates issued by this CA:
SHA256
SHA384
SHA512
SHA1
MD5
Allow administrator interaction when the private key is accessed by the CA.
More about Cryptography
< Previous
Next >
Configure
Cancel

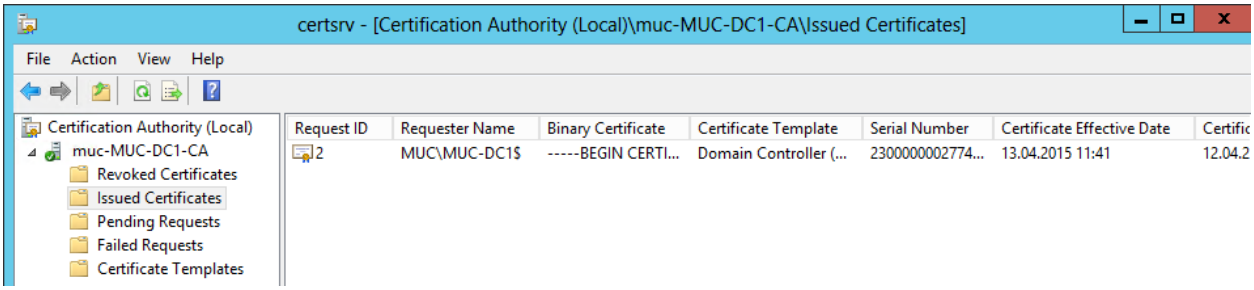

AD CS Configuration
CA Name
DESTINATION SERVER
MUC-DC1.muc.brcd.local
Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results
Specify the name of the CA
Type a common name to identify this certification authority (CA). This name is added to all certificates issued by the CA. Distinguished name suffix values are automatically generated but can be modified.
Common name for this CA:
muc-MUC-DC1-CA
Distinguished name suffix:
DC=muc,DC=brcd,DC=local
Preview of distinguished name:
CN=muc-MUC-DC1-CA,DC=muc,DC=brcd,DC=local
More about CA Name
< Previous
Next >
Configure
Cancel


AD CS Configuration
Validity Period
DESTINATION SERVER
MUC-DC1.muc.brcd.local
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):
20
Years
CA expiration Date: 13.04.2035 11:46:00
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


AD CS Configuration
Confirmation
DESTINATION SERVER
MUC-DC1.muc.brcd.local
Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results
To configure the following roles, role services, or features, click Configure.
Active Directory Certificate Services
Certification Authority
CA Type: Enterprise Root
Cryptographic provider: RSA#Microsoft Software Key Storage Provider
Hash Algorithm: SHA1
Key Length: 2048
Allow Administrator Interaction: Disabled
Certificate Validity Period: 13.04.2035 11:46:00
Distinguished Name: CN=muc-MUC-DC1-CA,DC=muc,DC=brcd,DC=local
Certificate Database Location: C:\Windows\system32\CertLog
Certificate Database Log Location: C:\Windows\system32\CertLog
< Previous
Next >
Configure
Cancel

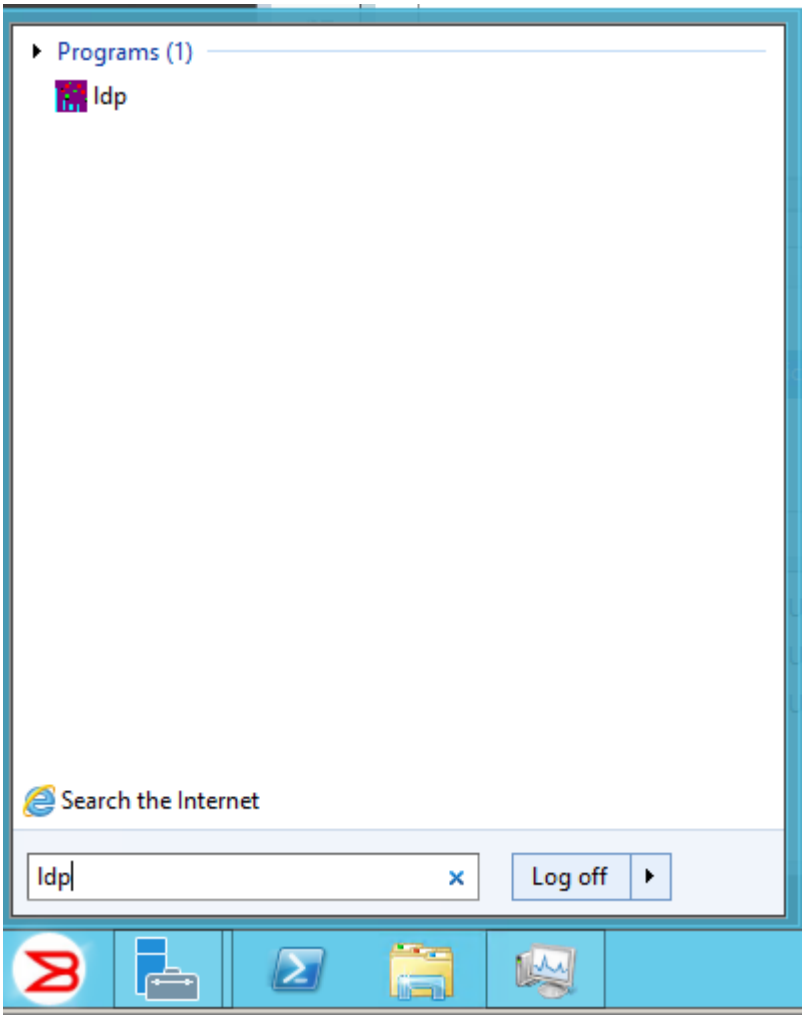


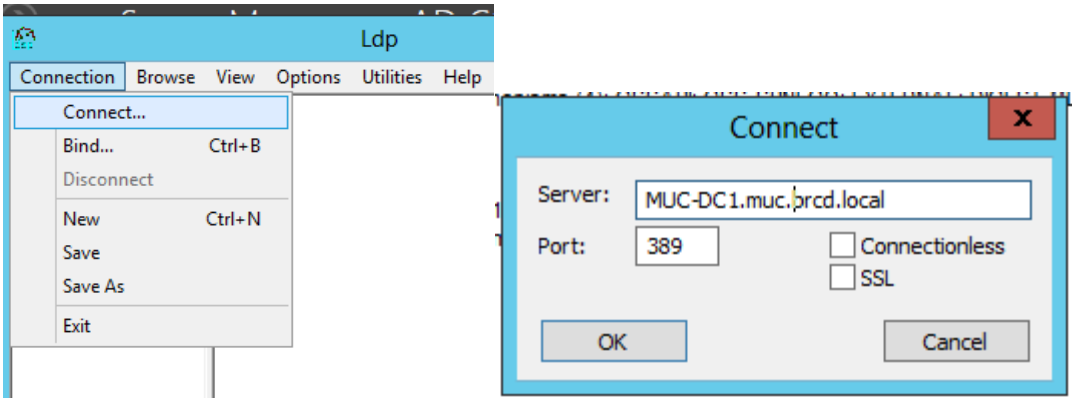
Check if the Root Certificate had been issued, in the Lab we had to reboot the server first:



Test TLS/SSL connectivity

Use the ldp.exe program from the Windows 2003 support tools and connect to the relevant Domain Controller:





When the connection has been established go to Options > TLS and select Start TLS. If LDAP is able to connect via TLS you receive:

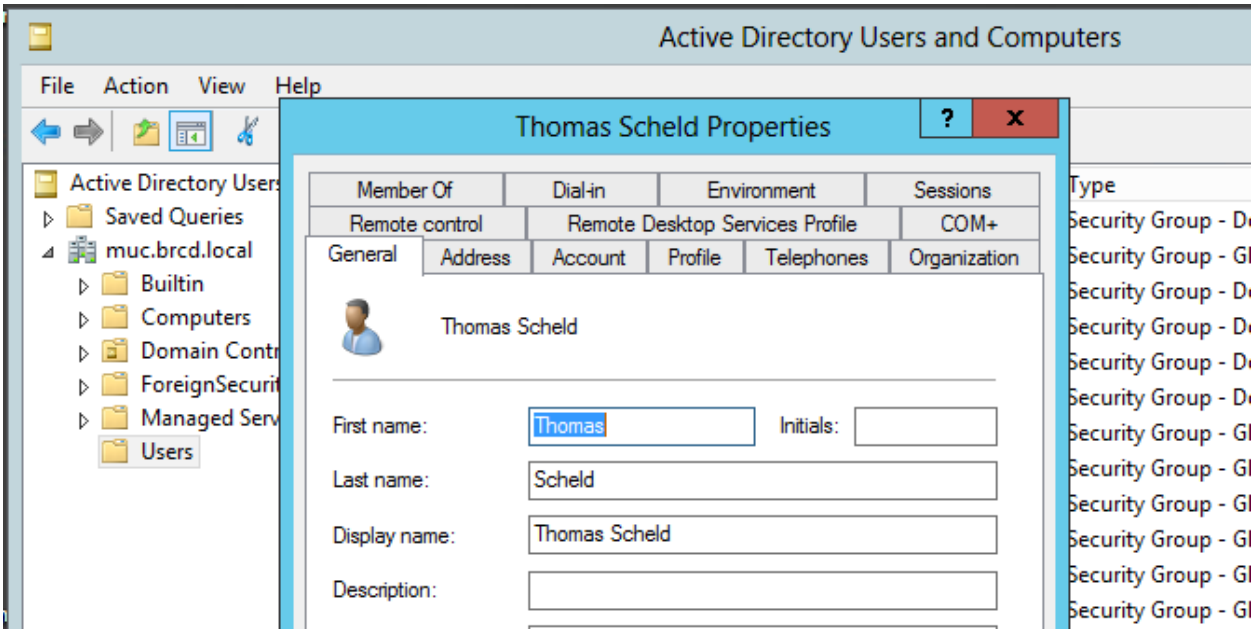
```
ldap_start_tls_s(ld, &retValue, result, SvrCtrls, ClntCtrls)
result <0>
```

Whereas a Domain Controller without valid certificate for authentication cannot use TLS:

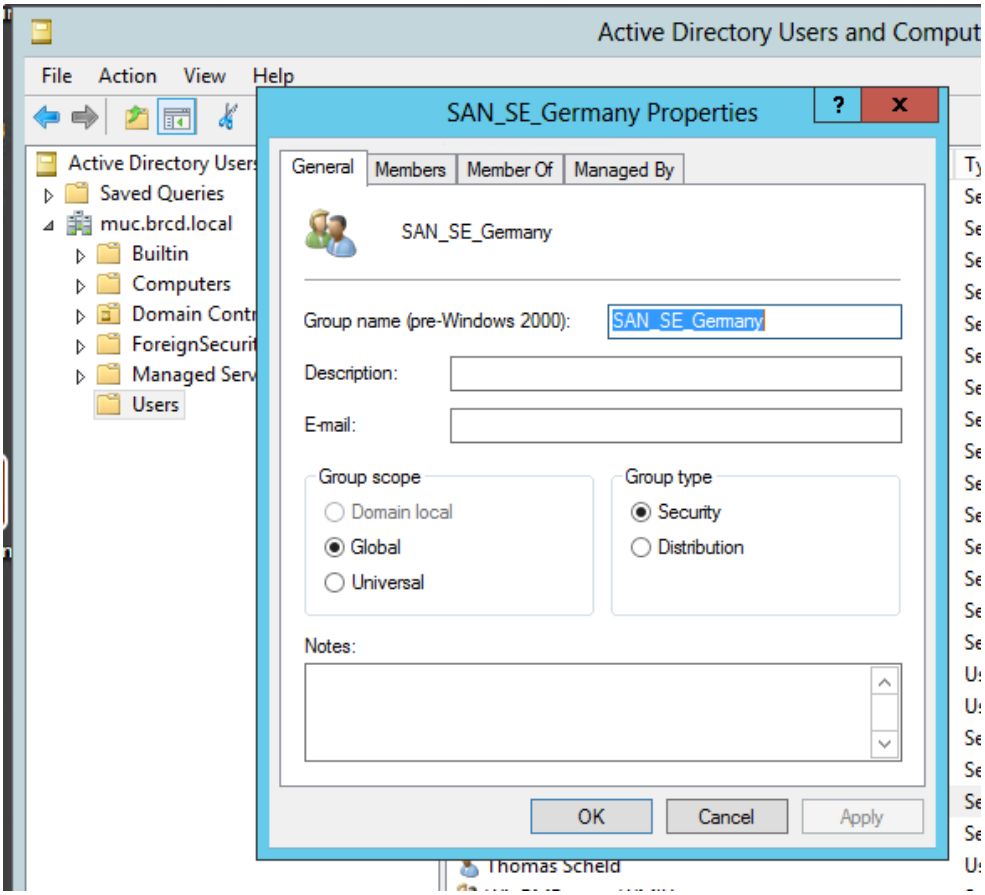
```
ldap_start_tls_s(ld, &retValue, result, SvrCtrls, ClntCtrls)

Error <0x50>:ldap_start_tls_s() failed: Other

Server Returned: 0x34: Unavailable

Server error: 00000000: LdapErr: DSID-0C090CF0, comment:
Error

initializing SSL/TLS, data 0, vece
```

If this test fails you cannot use this Domain Controller for LDAP authentication.

Create an AD User:



Create an AD Admin Group



To create a group in Active Directory, refer to www.microsoft.com or Microsoft documentation. You must verify that the group has the following attributes:

- The name of the group must match the RBAC role.
- The Group Type must be Security.
- The Group Scope must be Global.
- The primary group in the AD server should not be set to the group corresponding to the switch role. You can choose any other group.
- If the user you created is not a member of the Users OU, then the User Principal Name, in the format of "user@domain", is required to log in.

Configuring the switch

At least one LDAP server must be configured before you can enable LDAP service. You can configure the LDAP service even if it is disabled on the switch. You can configure up to five LDAP servers. You must be logged in as admin or switchAdmin to configure the LDAP service. The LDAP servers are contacted in the order they are listed, starting from the top of the list and moving to the bottom.

Configure LDAP Server and Domain

```
se-6510:FID128:admin>   aaaconfig   --add   172.27.180.100   -conf   ldap   -d
muc.brcd.local
se-6510:FID128:admin> aaaconfig --show
RADIUS CONFIGURATIONS
=====================
RADIUS configuration does not exist.

LDAP CONFIGURATIONS
===================
Position                : 1
Server                  : 172.27.180.100
Port                    : 389
Domain                  : muc.brcd.local
Timeout(s)              : 3

TACACS+ CONFIGURATIONS
======================
TACACS+ configuration does not exist.
Primary AAA Service: Switch database
Secondary AAA Service: None
```

Activate LDAP authentication as primary and switch database as secondary service

```
se-6510:FID128:admin> aaaconfig --authspec "ldap;local"
se-6510:FID128:admin> aaaconfig --show
RADIUS CONFIGURATIONS
=====================
RADIUS configuration does not exist.

LDAP CONFIGURATIONS
===================
Position                : 1
Server                  : 172.27.180.100
Port                    : 389
Domain                  : muc.brcd.local
Timeout(s)              : 3

Primary AAA Service: LDAP
Secondary AAA Service: Switch database
```

Map LDAP group to switch role

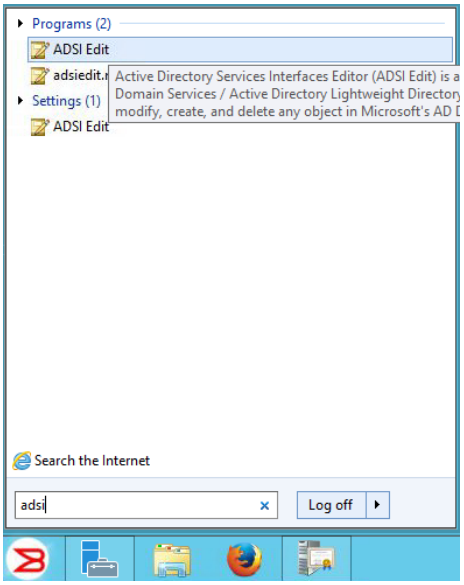
```
se-6510:FID128:admin> ldapcfg --maprole SAN_SE_Germany admin
LDAP role has been successfully mapped.
se-6510:FID128:admin> ldapcfg --show
        LDAP Role       |       Switch Role
------------------------------------------------
        SAN_SE_Germany  |       admin
```

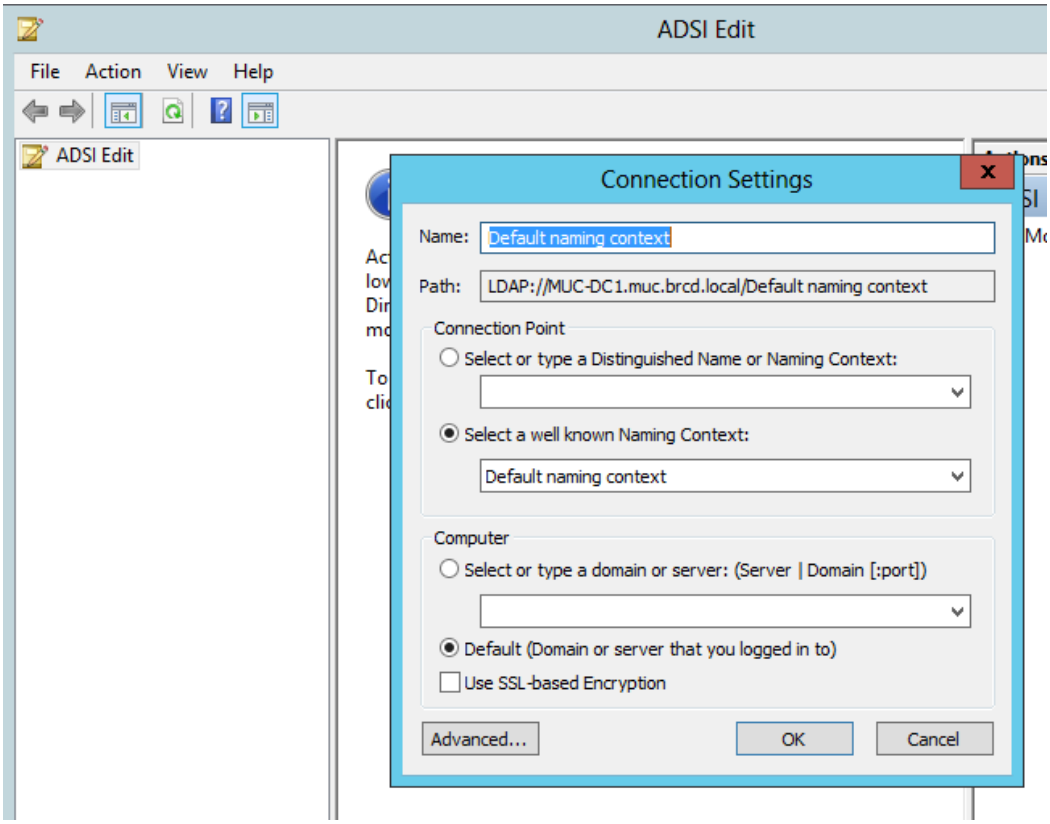
Test login using your AD/LDAP user account and password

```
login as: tscheld
tscheld@172.27.180.171's password:

se-6510:FID128:tscheld> userconfig --show
Account name: tscheld
Description: Remote Account
Enabled: Yes
Password Last Change Date: Unknown (UTC)
Password Expiration Date: Not Applicable (UTC)
Locked: No
Home LF Role: admin
Role-LF List: admin: 128
No chassis permission
Home LF: 128
```

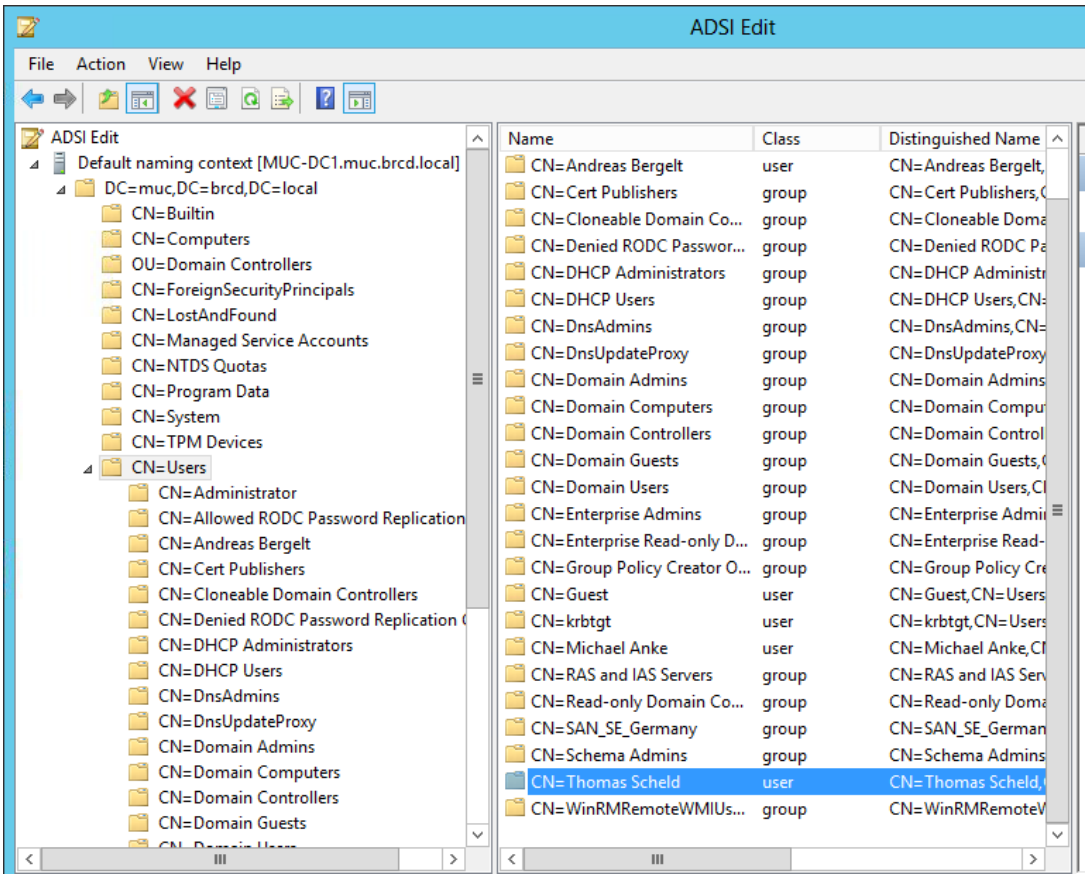
Configuration for Switches with virtual Fabrics enables

As seen in the previous output, the mapped users won't have chassis permission per default. In order to configure Admin Domains or Virtual Fabrics you have edit the advanced properties of the user object in Active Directory. You can use ADSI edit to do so:





Locate the user to change:



Click Properties and change the Attributes, locate “adminDescription” and change the values:

- If you are using Administrative Domains, enter the value of the Admin Domain separated by an underscore (_) into the Value field, example:

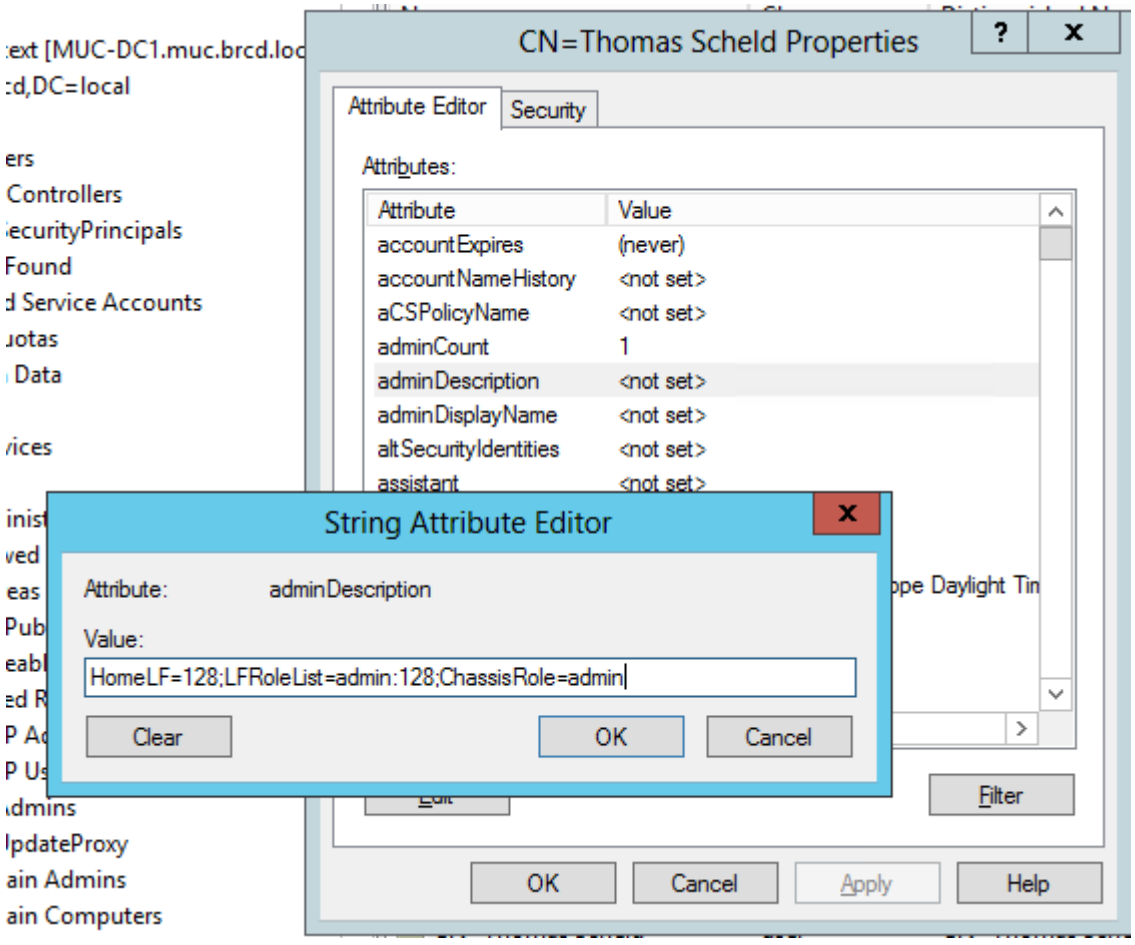
  ```
  adlist_0_10_200_endAd
  ```

  Home Admin Domain (homeAD) for the user will be the first value in the adlist (Admin Domain list). If a user has no values assigned in the adlist attribute, then the homeAD ‘0’ will be the default administrative domain for the user.

- If you are using Virtual Fabrics, enter the values of the logical fabrics separated by a semi-colon (;) into the Value field, example

```
HomeLF=10;LFRoleList=admin:128,10;ChassisRole=admin
```

In this example, the logical switch that would be logged in to by default is 10. If 10 is not available, then the lowest FID available will be chosen. You would have permission to enter logical switch 128 and 10 in an admin role and you would also have the chassis role permission of admin.



NOTE

You can perform batch operations using the Ldifde.exe utility. For more information on importing and exporting schemas, refer to your Microsoft documentation or visit www.microsoft.com.

In our example for a virtual fabrics enabled switch with no logical fabrics configured, the following value hat been configured:

```
HomeLF=128;LFRoleList=admin:128;ChassisRole=admin
```

Checking the login now:

```
login as: tscheld

tscheld@172.27.180.171's password:

se-6510:FID128:tscheld> userconfig --show


Account name: tscheld

Description: Remote Account

Enabled: Yes

Password Last Change Date: Unknown (UTC)

Password Expiration Date: Not Applicable (UTC)

Locked: No

Home LF Role: admin

Role-LF List: admin: 128

Chassis Role: admin

Home LF: 128
```