

# MiVoice MX-ONE

## Configuration of AD LDS - User Guide

Release 7.1

March 5, 2019



## Notice

The information contained in this document is believed to be accurate in all respects but is not warranted by **Mitel Networks™ Corporation (MITELE<sup>®</sup>)**. The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes. No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

## Trademarks

The trademarks, service marks, logos and graphics (collectively "Trademarks") appearing on Mitel's Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC) or its subsidiaries (collectively "Mitel") or others. Use of the Trademarks is prohibited without the express consent from Mitel. Please contact our legal department at [legal@mitel.com](mailto:legal@mitel.com) for additional information. For a list of the worldwide Mitel Networks Corporation registered trademarks, please refer to the website: <http://www.mitel.com/trademarks>.

® , ™ Trademark of Mitel Networks Corporation  
© Copyright 2019, Mitel Networks Corporation  
All rights reserved

---

# Contents

<b>Chapter: 1</b>	<b>Introduction . . . . .</b>	<b>1</b>
	General Introduction to AD LDS in MiVoice MX-ONE 6.x . . . . .	1
	About this guide . . . . .	1
	Requirements . . . . .	1
	Steps for Getting Started with AD LDS . . . . .	1
 <b>Chapter: 2</b>	 <b>Prerequisite . . . . .</b>	 <b>3</b>
	Enabling AD LDS in Windows Server . . . . .	3
	Creating AD LDS Instance . . . . .	10
	Creating the Custom LDF File to suit for AD LDS Setup . . . . .	20
	Restarting the AD LDS Instance . . . . .	24
	Creating an Admin User in AD LDS . . . . .	25
	Checking User Authentication . . . . .	33
	Adding Attributes to UserProxyFull Class . . . . .	35
	Editing Object (UserProxyFull) Class as User Object Class . . . . .	40
	Modifying MS-AdamSyncConf File . . . . .	44
	Synchronizing Users from Active Directory to AD LDS Instance . . . . .	45
	Checking Synchronized Users in AD LDS . . . . .	45
	Enabling LDAPS (SSL) for AD LDS in Window Server . . . . .	46
	Using AD LDS as a User Repository in PM Application . . . . .	53
	Enabling SSL for PM Application . . . . .	56
	Enabling AD Authentication in PM Located Server . . . . .	57
	Uninstalling AD LDS Instance and AD LDS Roles from Server . . . . .	57

# Introduction

## General Introduction to AD LDS in MiVoice MX-ONE 6.x

Active Directory Lightweight Directory Services (AD LDS) role, is formerly known as Active Directory Application Mode (ADAM). Any user can provide directory services for directory-enabled applications without incurring the overhead of domains and forests and the requirements of a single schema throughout a forest.

It is a Lightweight Directory Access Protocol (LDAP) directory service that provides data storage and retrieval support for directory-enabled applications, without the dependencies that are required for the Active Directory Domain Services (AD DS). You can run multiple instances of AD LDS concurrently on a single computer, with an independently managed schema for each AD LDS instance.

## About this guide

This guide describes the processes for setting up AD LDS and getting it running. You can use the procedures in this guide to configure AD LDS on servers that are running the Windows Server® 2012 operating system.

## Requirements

Before you start using the procedures in this guide, do the following:

- 1) Check the availability of at least one test computer on which you can install AD LDS.
- 2) Log on to Windows Server 2008 with an administrator account.

## Steps for Getting Started with AD LDS

The following sections provide step-by-step instructions for setting up AD LDS. These sections provide both graphical user interface (GUI) and command-line methods for configuration setup of AD LDS.

- 1) Enabling AD LDS in Windows Server
- 2) Creating AD LDS Instance
- 3) Restarting the AD LDS Instance
- 4) Creating an Admin User in AD LDS
- 5) Checking User authentication
- 6) Adding Attributes to UserProxyFull Class
- 7) Editing UserProxyFull Object Class as User Object class
- 8) Modifying MS-AdamSyncConf File
- 9) Synchronizing Users from Active Directory to AD LDS Instance



- 10) Checking Synchronized Users in ADLDS
- 11) Enabling LDAPS (SSL) for AD LDS
- 12) Using AD LDS as a User repository in Provisioning Manager (PM) Application
- 13) Uninstalling of AD LDS Instance and AD LDS Roles from Server

**NOTE:** *To maximize your chances of successfully completing the objectives of this guide, it is important that you follow the steps in this guide in the order in which they are presented.*

# Prerequisite

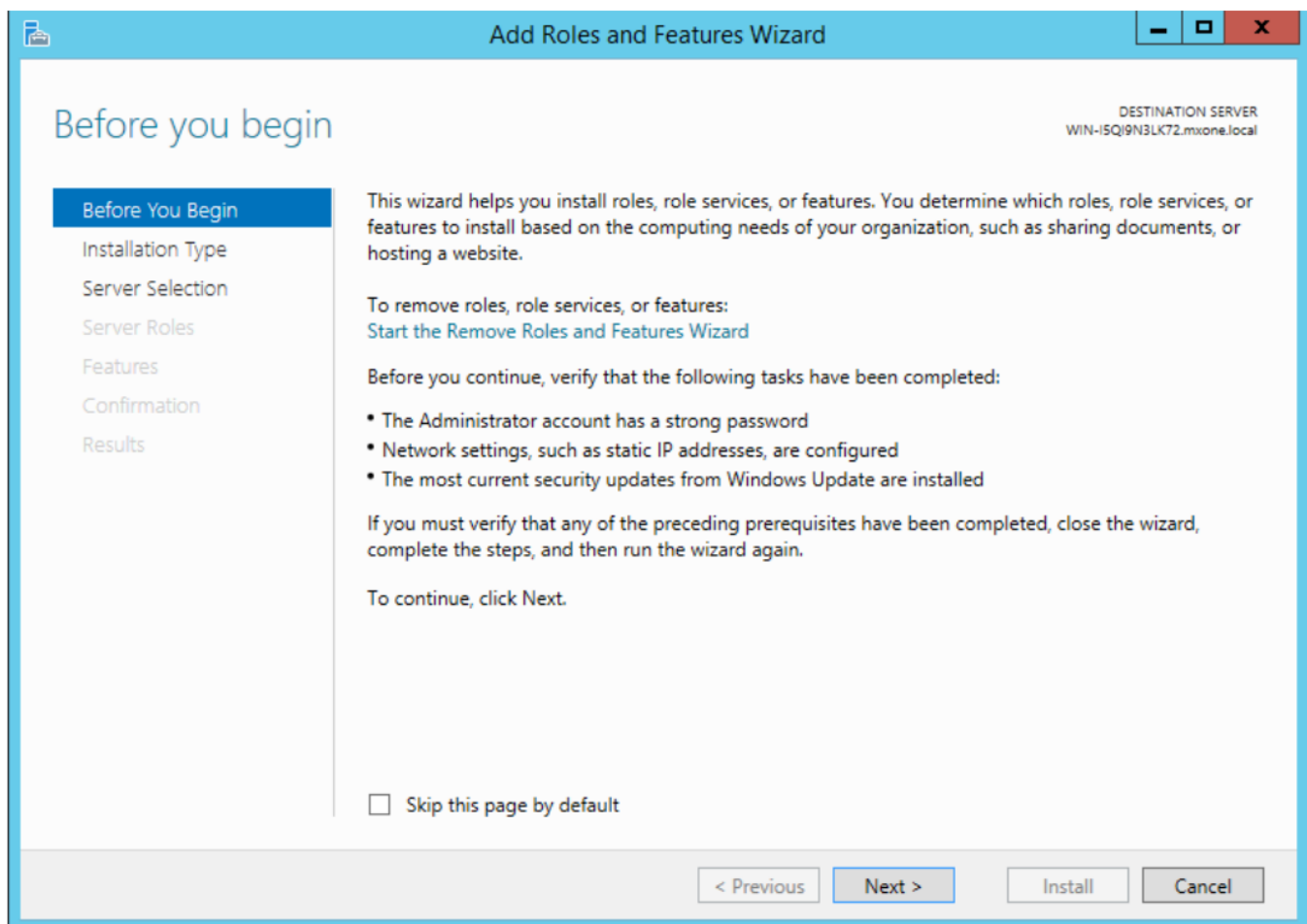
AD LDS server should be a part of Active Directory Domain, so that users can login into AD LDS server using their respective User IDs and Passwords from active directory. User display name and User ID must be same in Active Directory created for all users.

## Enabling AD LDS in Windows Server

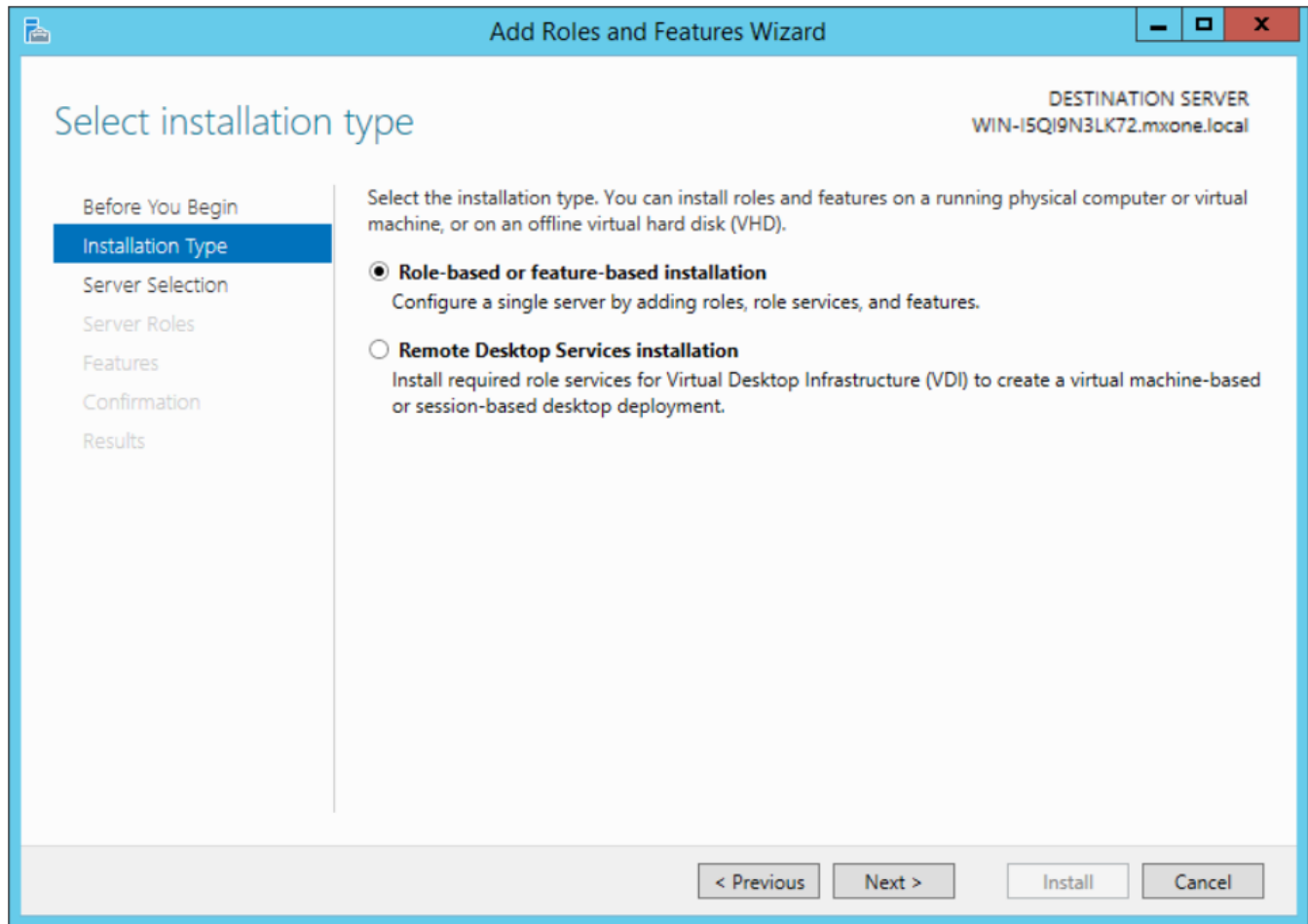
If any of the organization wants to use AD LDS as a proxy to AD Server, then they can follow this document to enable AD LDS as a proxy server.

To enable AD LDS in Window Server, do the following:

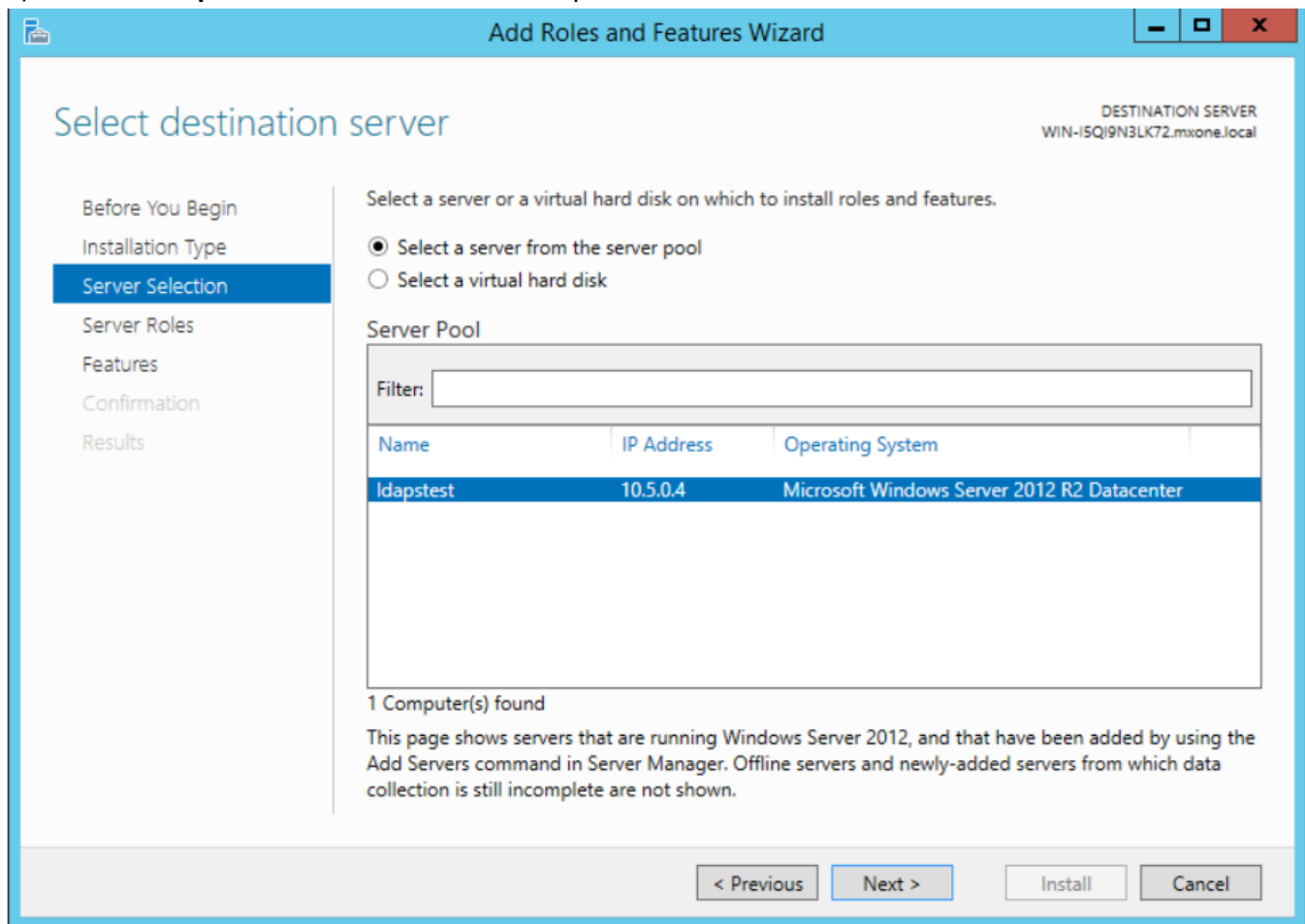
- 1) Click **Start**, and then click **Server Manager**. You can do this from Task Bar or from **Start/ Administrative Tools** menu.
- 2) Select the **Server Manager > Add Roles and Features**. Click **Next**. The following screen appears.



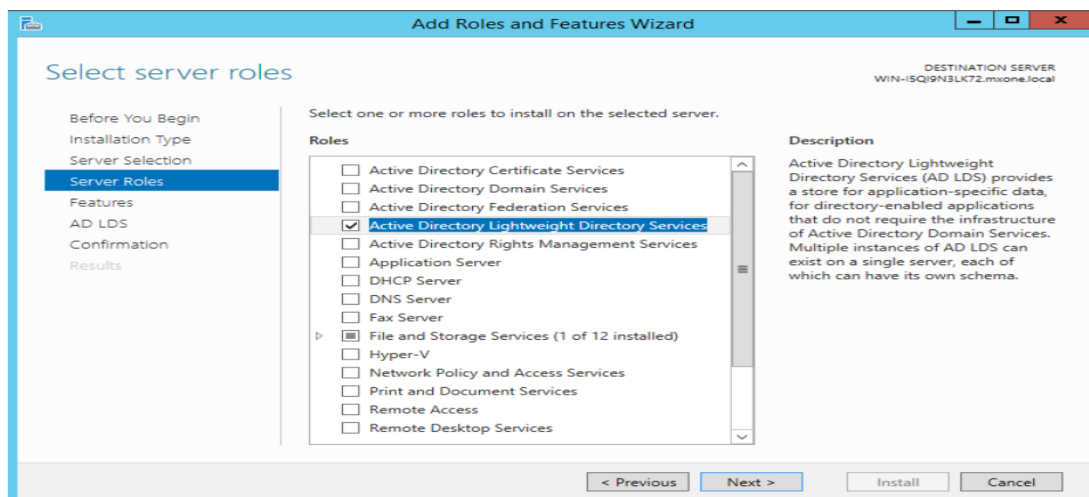
- 3) Choose **Role-based or feature-based installation**. Click **Next**.



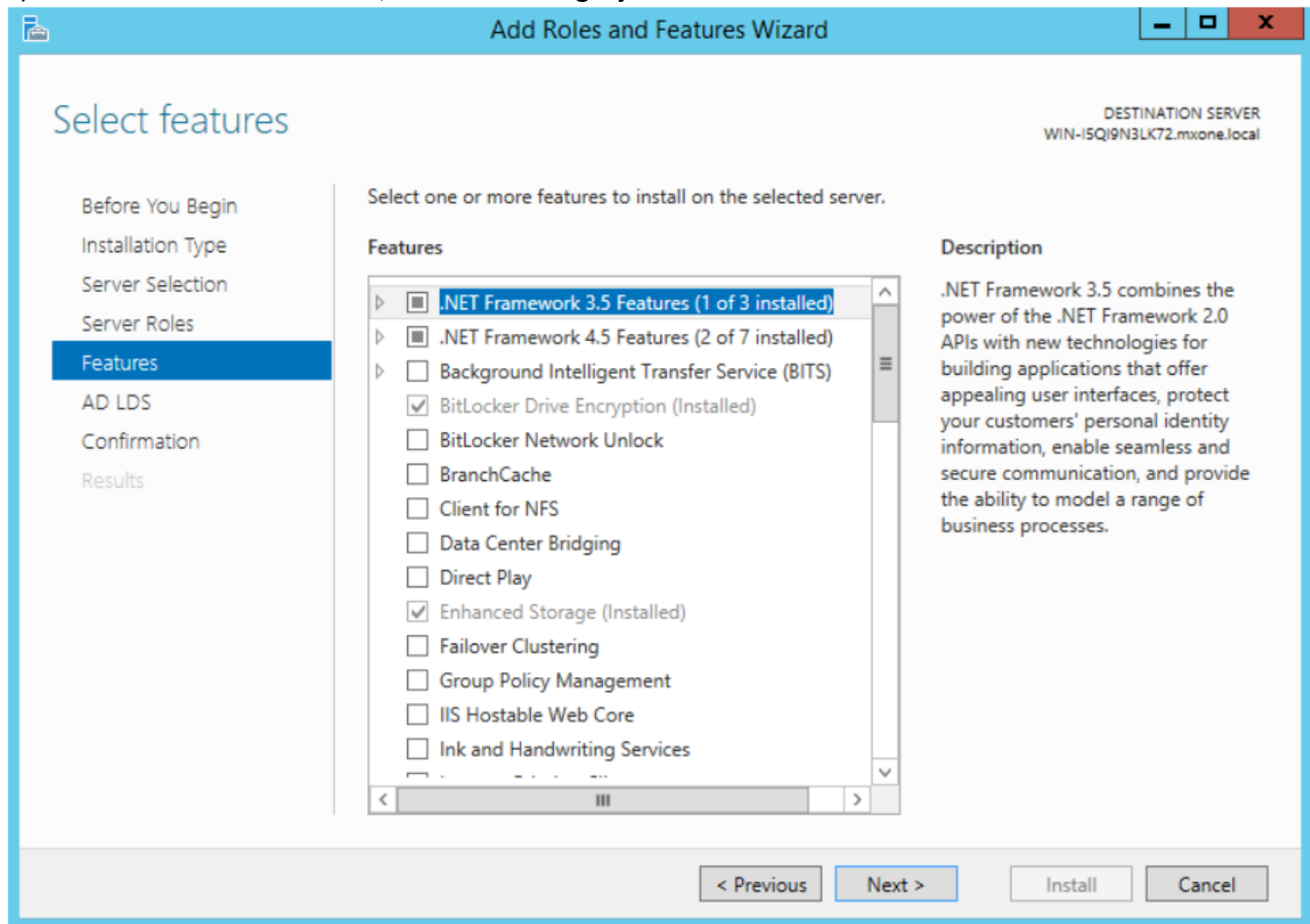
- 4) Select **ldapstest** server from the server pool. Click **Next**



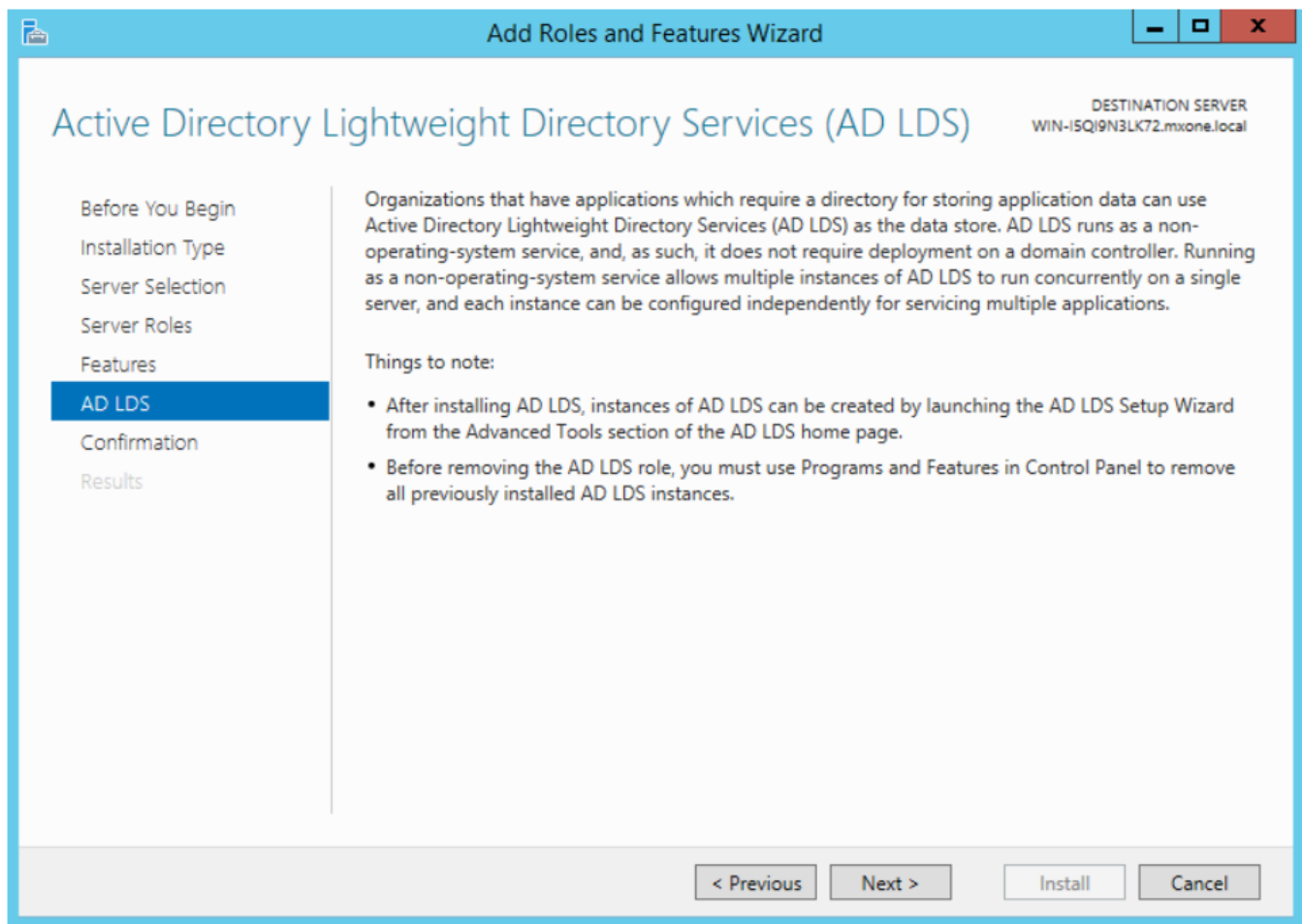
- 5) Mark **Active Directory Lightweight Directory Services** from the list of roles and click **Next**.



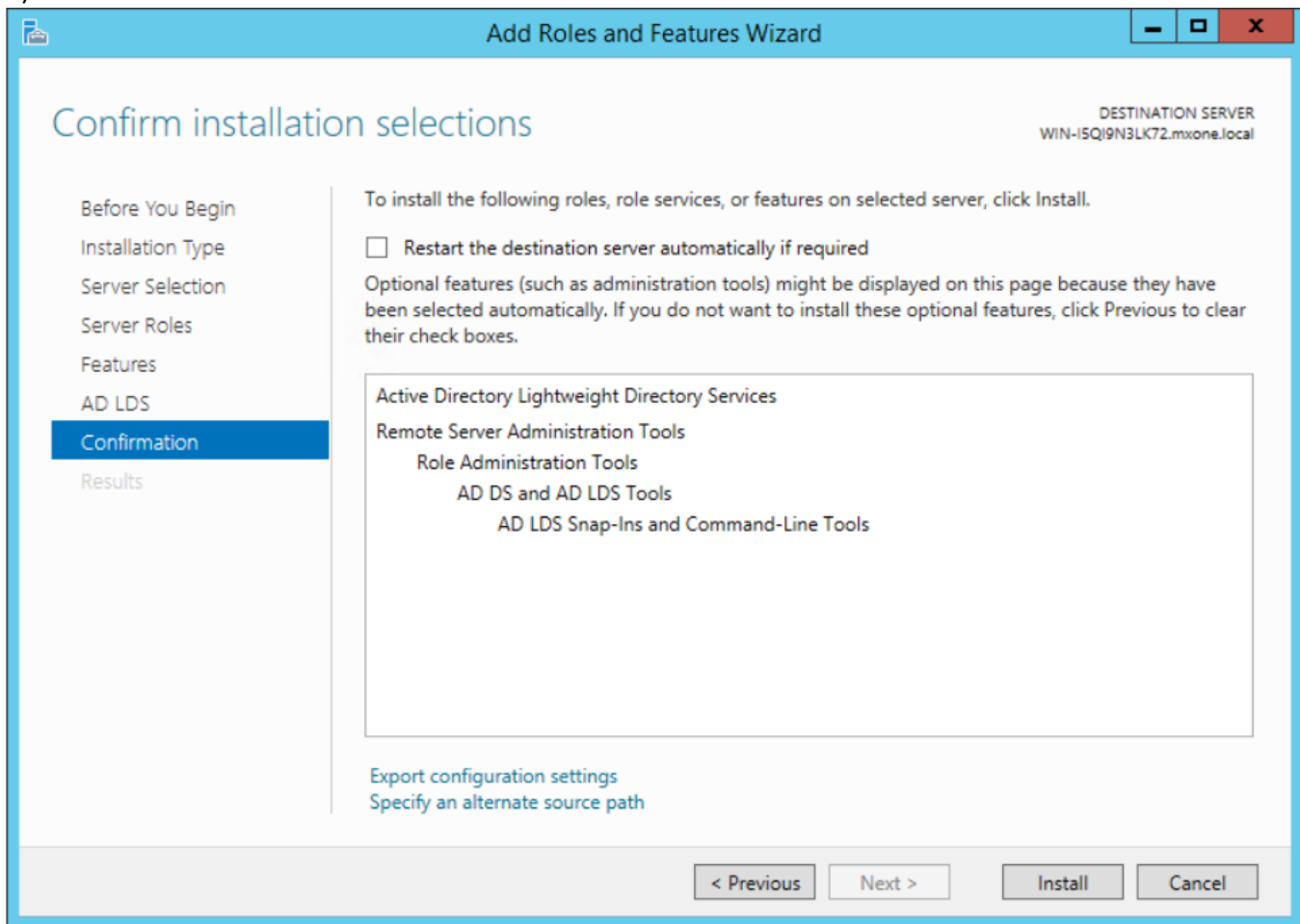
6) From the list of features, choose nothing – just click **Next**



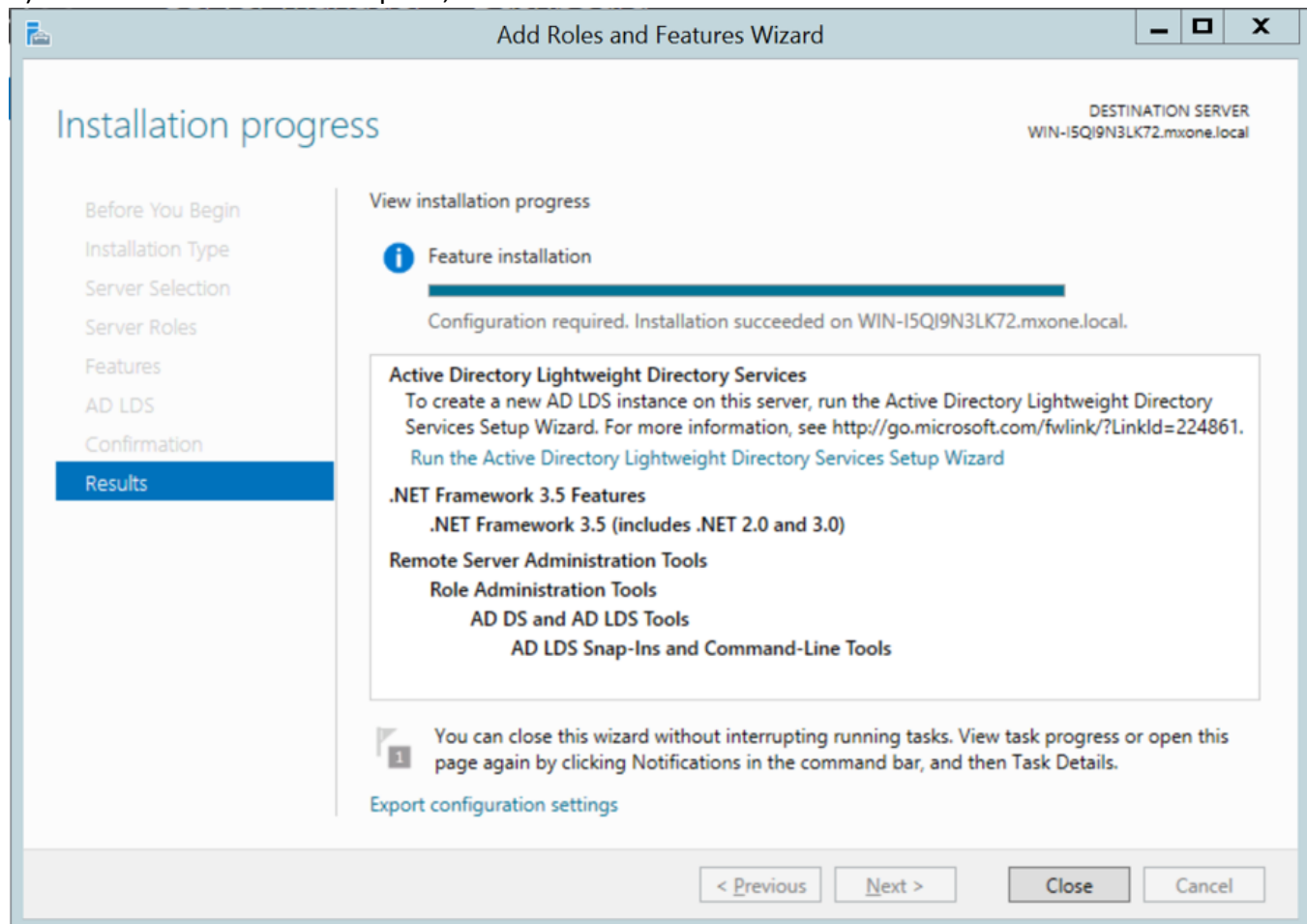
7) click **Next**.



8) Click **Install** to start installation.



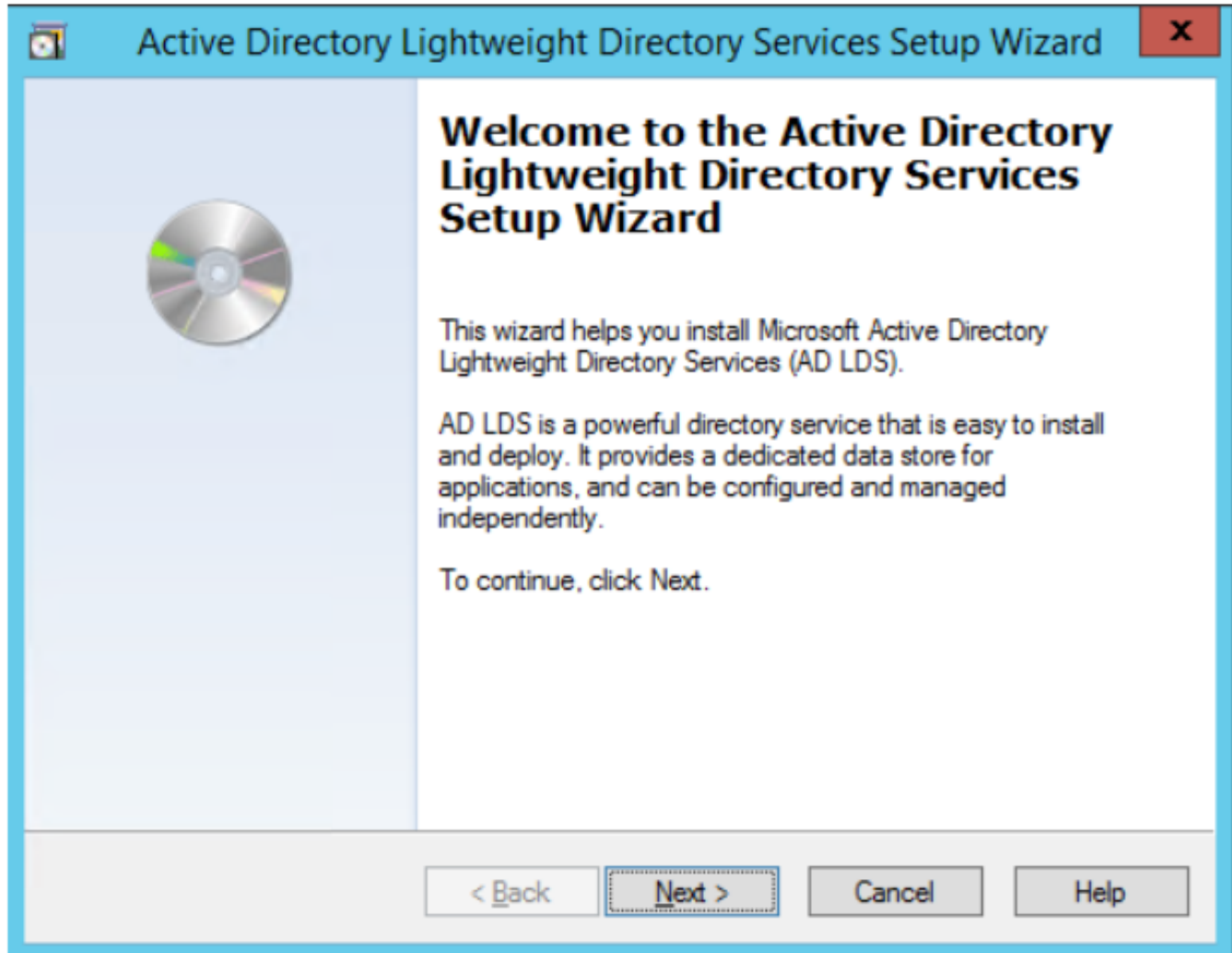
- 9) Once installation is complete, click **Close**.



- 10) **NOTE:** AD LDS Role is successfully set up. Create a new AD LDS Instance as “Instance1” using the wizard.



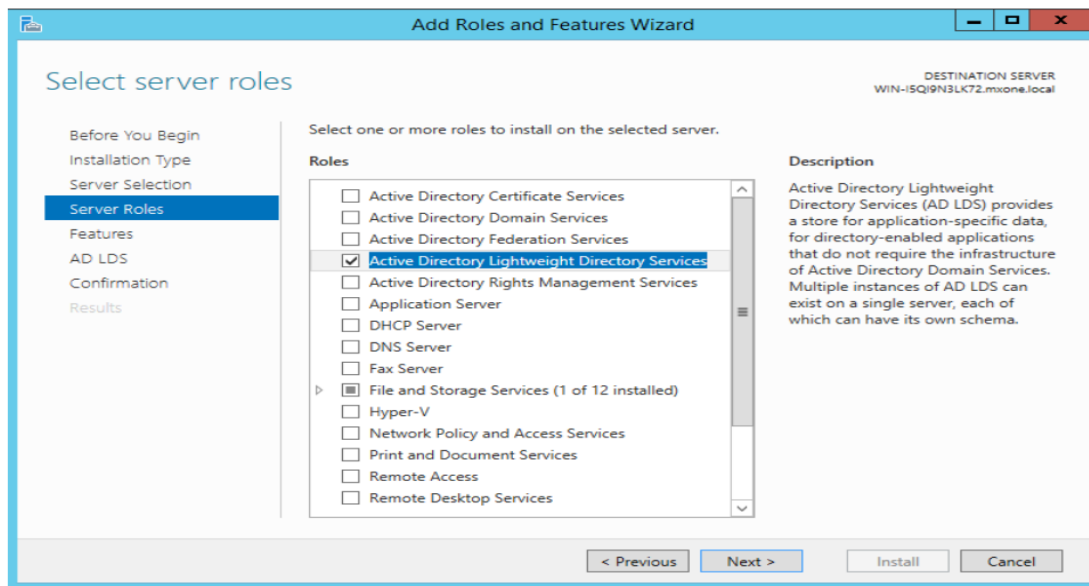
- 11) Click the Run the **Active Directory Lightweight Directory Services Setup Wizard** shown in the above screen. And then click **Close**.



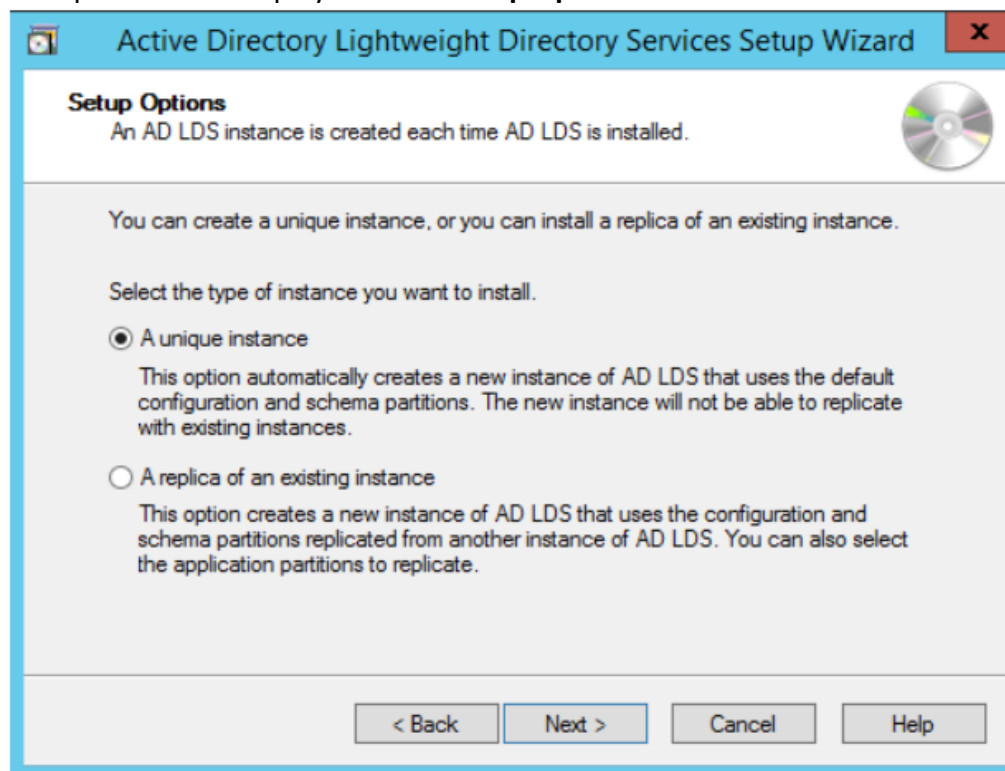
*NOTE: This entire procedure implemented and documented based on Windows 2012 edition.*

## Creating AD LDS Instance

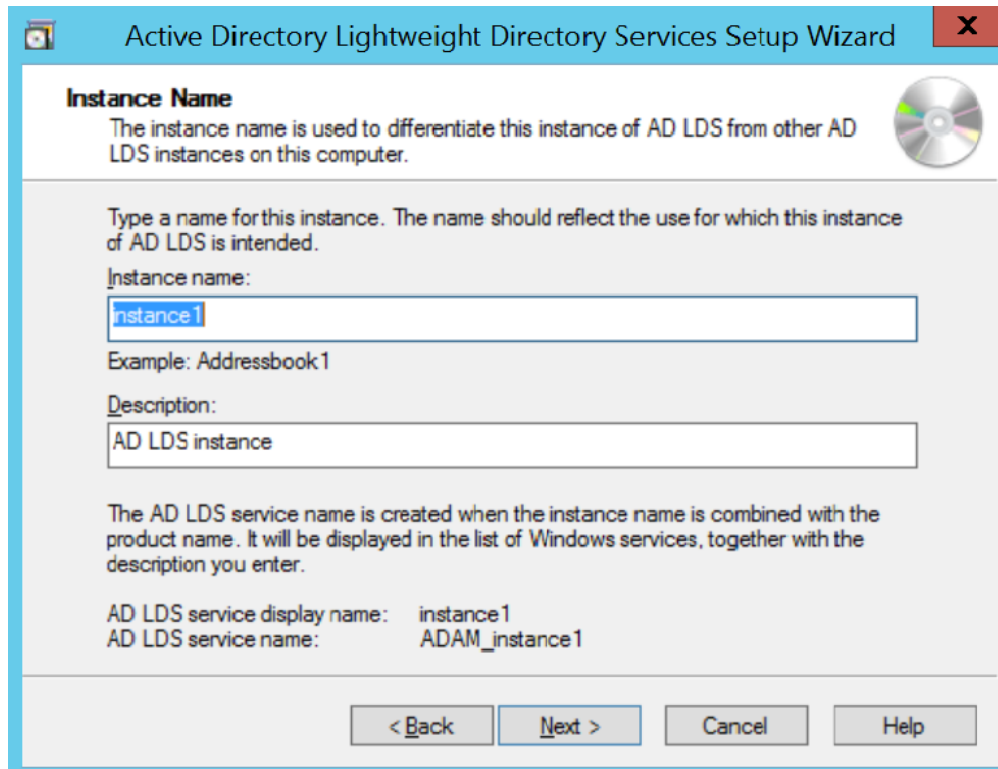
- 1) Open **Server Manager**.
- 2) In the Console tree, select **Roles**> select **Active Directory Lightweight Directory Services** from **Roles Summary** section.



- 3) Click **Next> Next...** until the AD LDS Role is successfully setup. Refer the step 10 and 11 of [Enabling AD LDS in Windows Server](#).
- 4) Select A unique instance displayed in the **Setup Options**. Click **Next**.



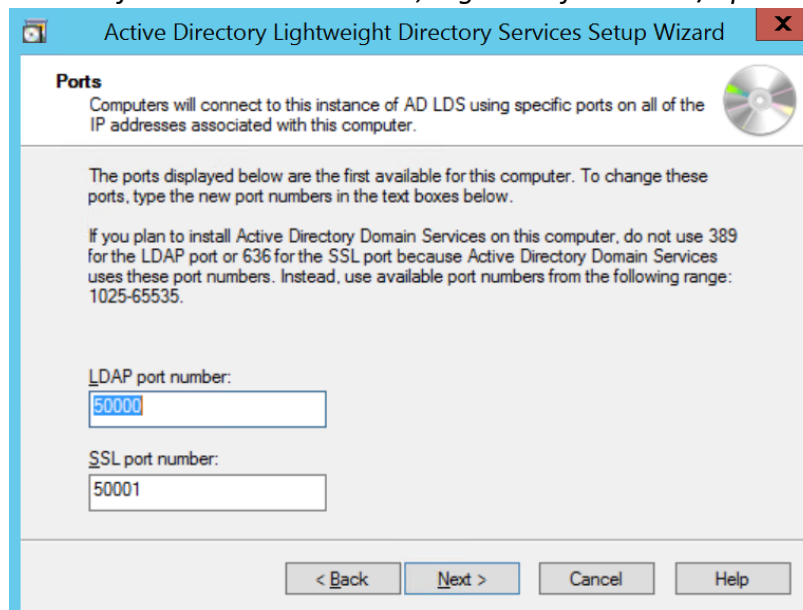
- 5) Enter the **Instance name** and **Description**. Click **Next**.



The screenshot shows the 'Instance Name' screen of the Active Directory Lightweight Directory Services Setup Wizard. The title bar reads 'Active Directory Lightweight Directory Services Setup Wizard'. The main heading is 'Instance Name'. Below it, a text box explains: 'The instance name is used to differentiate this instance of AD LDS from other AD LDS instances on this computer.' To the right is a CD icon. The instructions state: 'Type a name for this instance. The name should reflect the use for which this instance of AD LDS is intended.' There are two text input fields: 'Instance name:' with 'instance1' entered, and 'Description:' with 'AD LDS instance' entered. Below these, an example is given: 'Example: Addressbook1'. Further down, it says: 'The AD LDS service name is created when the instance name is combined with the product name. It will be displayed in the list of Windows services, together with the description you enter.' At the bottom, it shows the resulting names: 'AD LDS service display name: instance1' and 'AD LDS service name: ADAM\_instance1'. At the very bottom are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'.

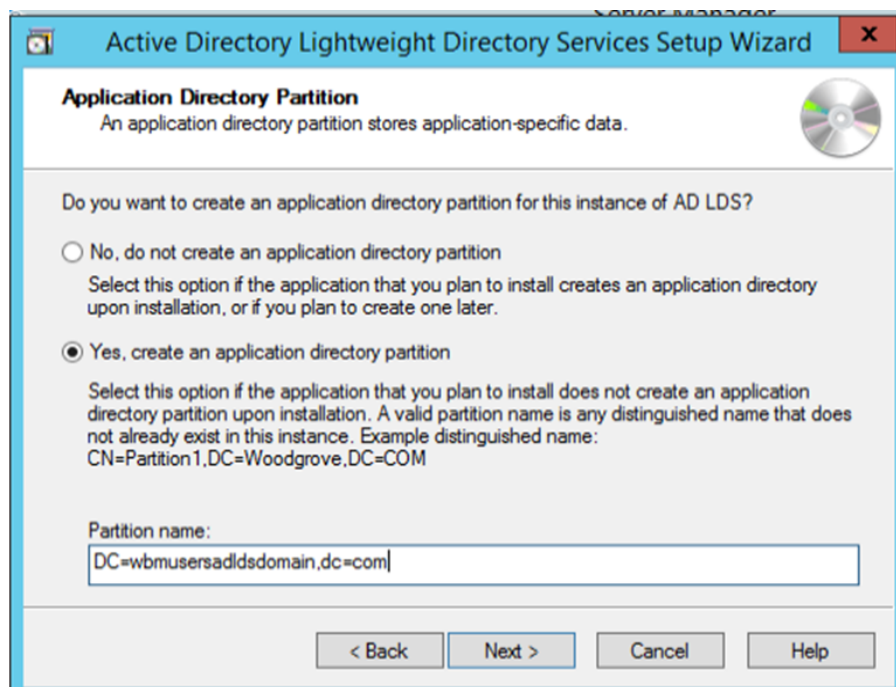
- 6) Enter the **LDAP port number** and **LDAPS SSL port number** that should be accessed from other applications to AD LDS; Or,
- 7) Click Next and continue with default ports.

**NOTE:** If you are installing AD LDS in the same server where Active Directory is installed, then it changes the port series from 50000. Otherwise, it gives default LDAP/s port such as 389, 636.

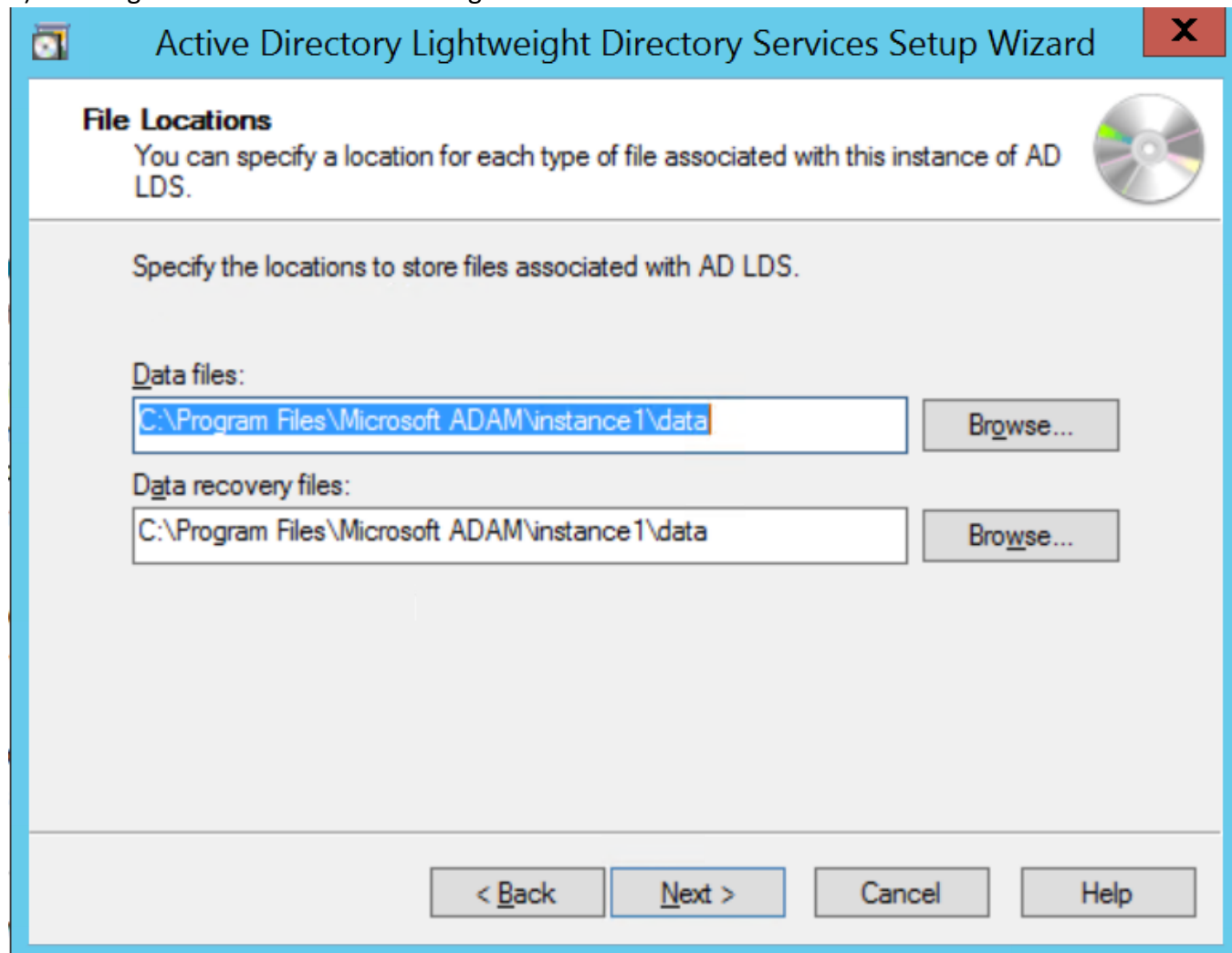


The screenshot shows the 'Ports' screen of the Active Directory Lightweight Directory Services Setup Wizard. The title bar reads 'Active Directory Lightweight Directory Services Setup Wizard'. The main heading is 'Ports'. Below it, a text box explains: 'Computers will connect to this instance of AD LDS using specific ports on all of the IP addresses associated with this computer.' To the right is a CD icon. The instructions state: 'The ports displayed below are the first available for this computer. To change these ports, type the new port numbers in the text boxes below.' A note follows: 'If you plan to install Active Directory Domain Services on this computer, do not use 389 for the LDAP port or 636 for the SSL port because Active Directory Domain Services uses these port numbers. Instead, use available port numbers from the following range: 1025-65535.' There are two text input fields: 'LDAP port number:' with '50000' entered, and 'SSL port number:' with '50001' entered. At the bottom are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'.

- 8) Select **Yes**, create and application directory partition and enter the Partition name. Click **Next**.



- 9) Using the default values for storage location of AD LDS files. Click **Next**.



The screenshot shows the 'Active Directory Lightweight Directory Services Setup Wizard' window. The title bar includes a close button (X). The window has a blue header bar with the title. Below the header, the 'File Locations' section is highlighted. It contains the text: 'You can specify a location for each type of file associated with this instance of AD LDS.' and a CD icon. Below this, the instruction 'Specify the locations to store files associated with AD LDS.' is displayed. There are two input fields: 'Data files:' and 'Data recovery files:'. Both fields contain the default path 'C:\Program Files\Microsoft ADAM\instance 1\data'. To the right of each field is a 'Browse...' button. At the bottom of the window, there are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'.

**Active Directory Lightweight Directory Services Setup Wizard**

**File Locations**  
You can specify a location for each type of file associated with this instance of AD LDS.

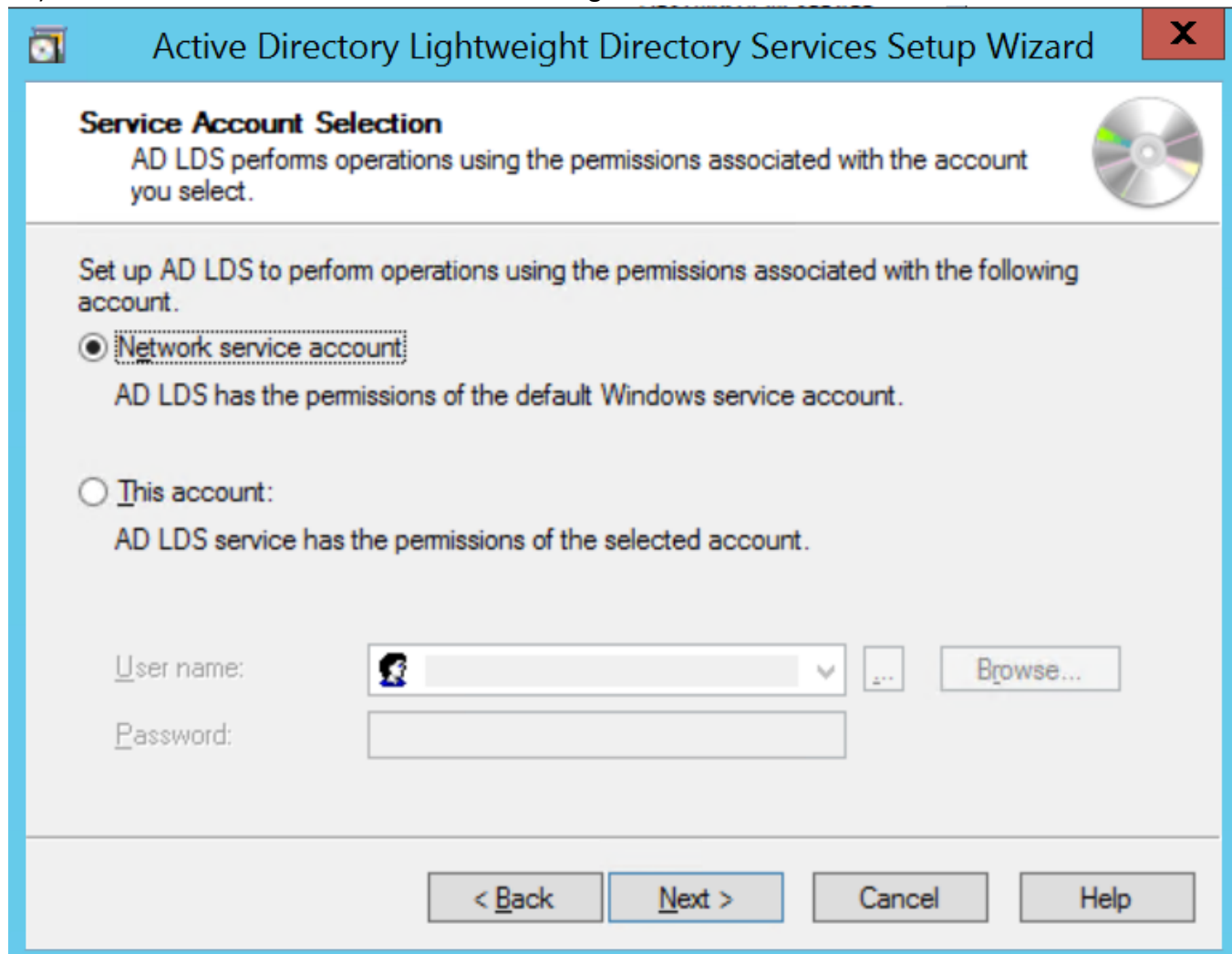
Specify the locations to store files associated with AD LDS.

Data files:  
C:\Program Files\Microsoft ADAM\instance 1\data Browse...

Data recovery files:  
C:\Program Files\Microsoft ADAM\instance 1\data Browse...

< Back Next > Cancel Help

10) Choose Network service account for running the AD LDS Service.



The image shows the 'Active Directory Lightweight Directory Services Setup Wizard' window. The title bar is blue with a close button (X) on the right. The main window has a light blue header bar with the title 'Active Directory Lightweight Directory Services Setup Wizard'. Below the header, the title 'Service Account Selection' is displayed in bold. A sub-header states: 'AD LDS performs operations using the permissions associated with the account you select.' To the right of this text is a CD icon. The main content area is light gray and contains the following text: 'Set up AD LDS to perform operations using the permissions associated with the following account.' Below this, there are two radio button options. The first option is 'Network service account', which is selected (indicated by a filled circle). Below this option, it says 'AD LDS has the permissions of the default Windows service account.' The second option is 'This account:', which is unselected (indicated by an empty circle). Below this option, it says 'AD LDS service has the permissions of the selected account.' At the bottom of the main content area, there are two input fields. The first is labeled 'User name:' and contains a dropdown menu with a user icon and a 'Browse...' button. The second is labeled 'Password:' and is an empty text box. At the bottom of the window, there are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'.


**Service Account Selection**

AD LDS performs operations using the permissions associated with the account you select.

Set up AD LDS to perform operations using the permissions associated with the following account.

☒ **Network service account**  
AD LDS has the permissions of the default Windows service account.

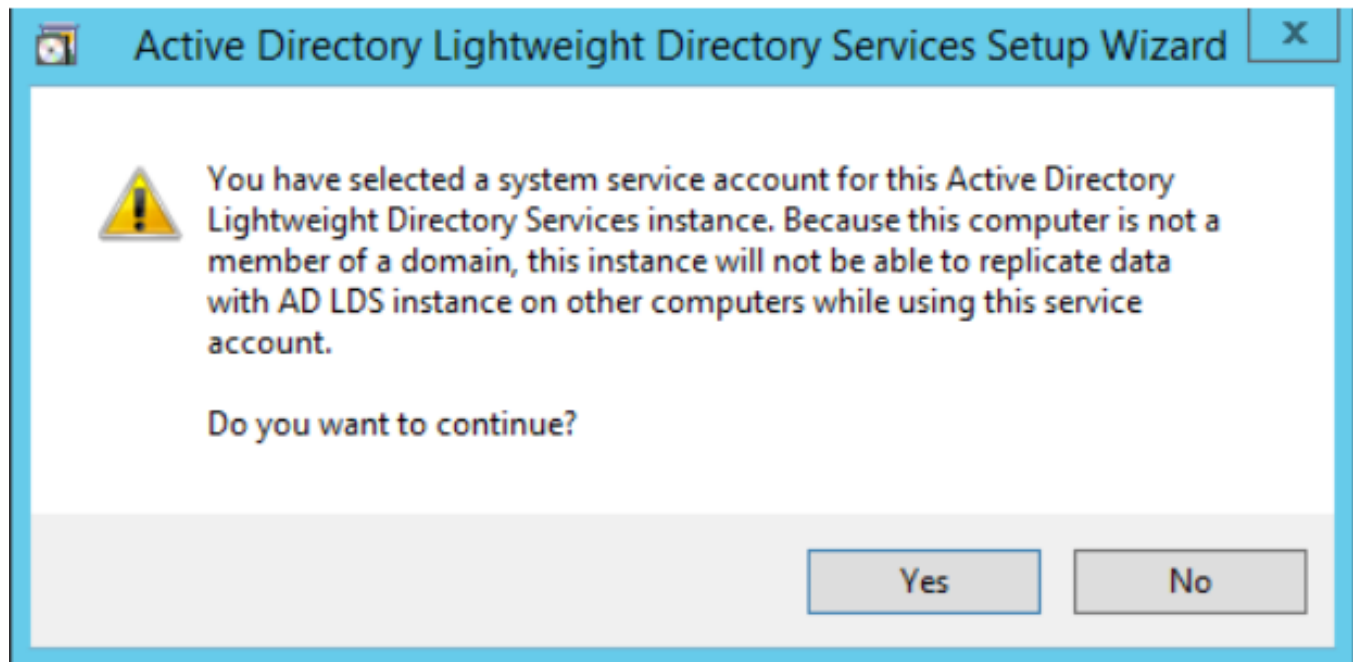
☐ **This account:**  
AD LDS service has the permissions of the selected account.

User name: 

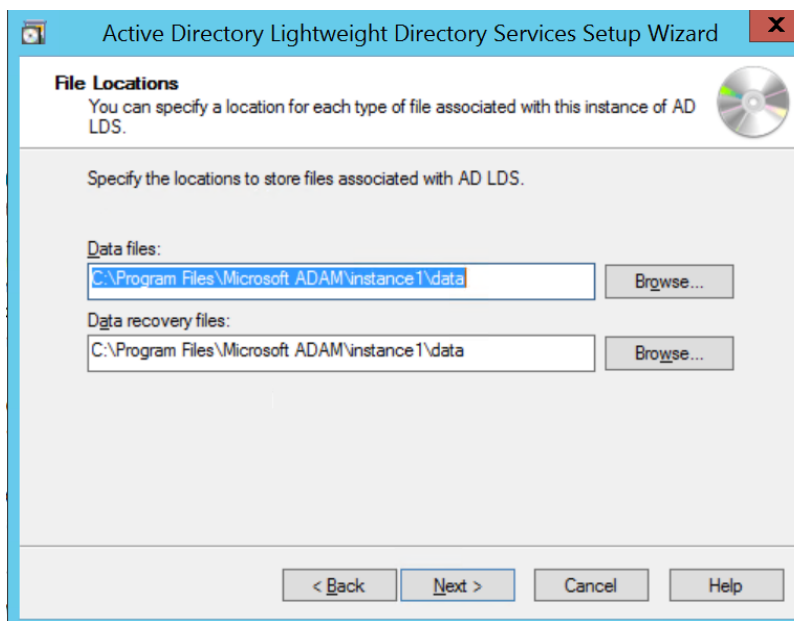
Password:

< Back Next > Cancel Help

- 11) You will receive a prompt warning about data replication. Since you are using a single LDAP Server, click **Yes**.

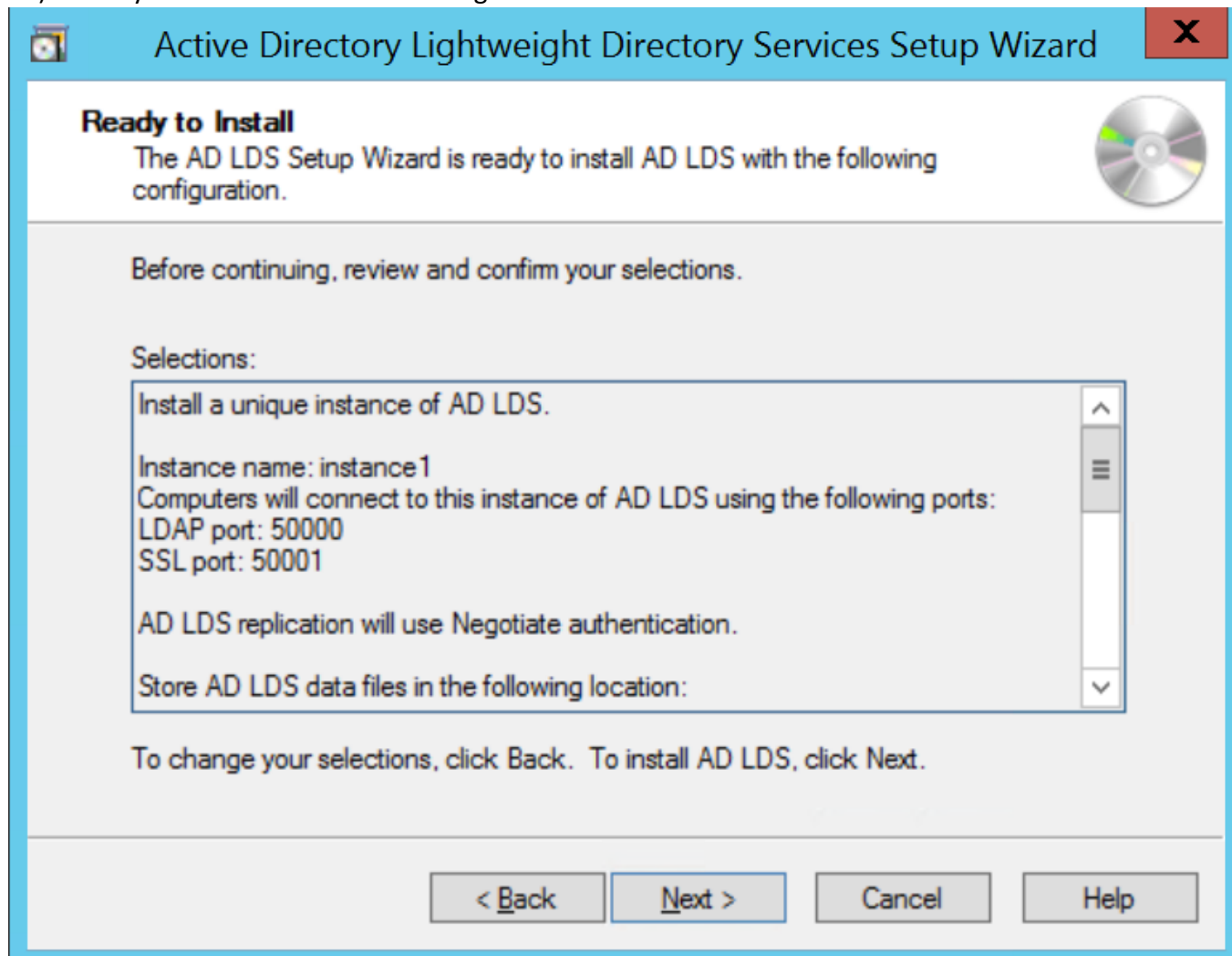


- 12) Select the below 3 LDF files from the Importing LDIF Files window.

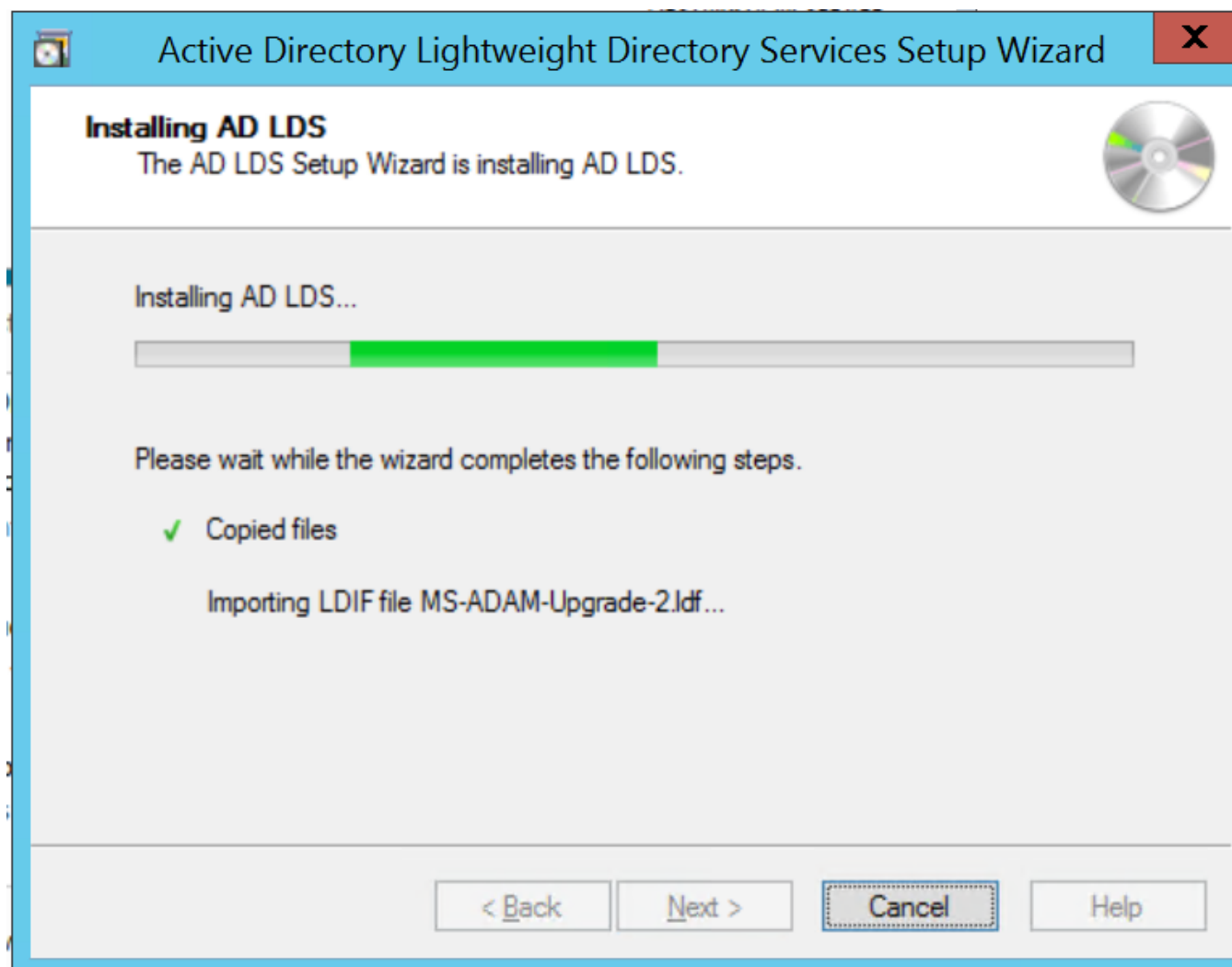


- a) **MS-InetOrgPerson.LDF**
- b) **MS-User.LDF**
- c) **MS-UserProxyFull.LDF**

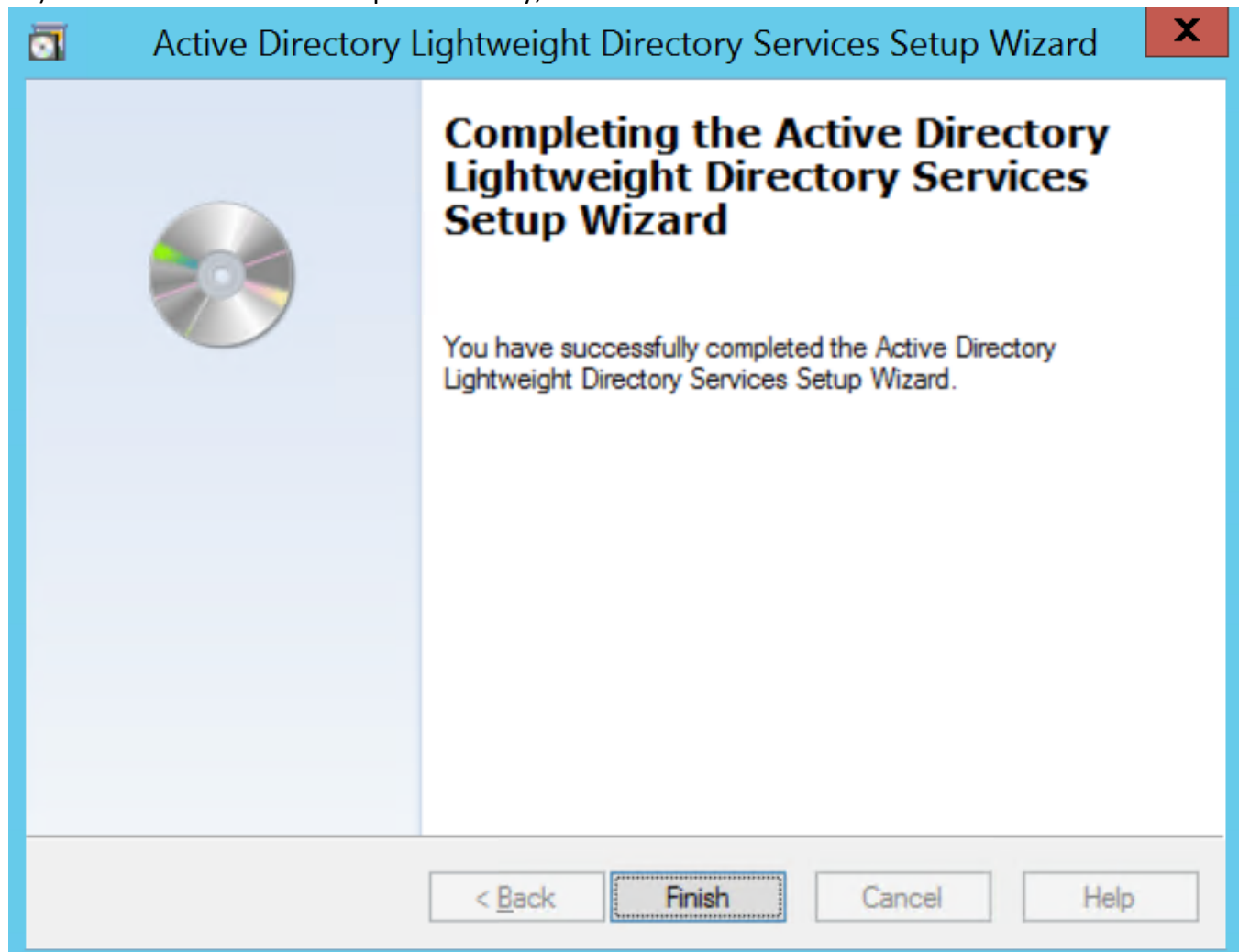
- 13) Verify that all the selections are right and then Click **Next** to confirm Installation.



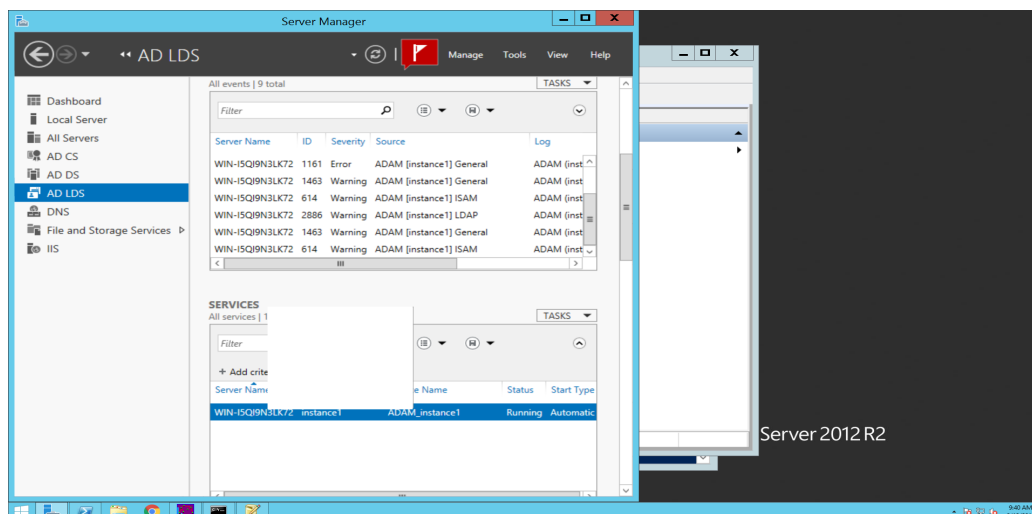




- 14) Once the instance is setup successfully, click **Finish**.

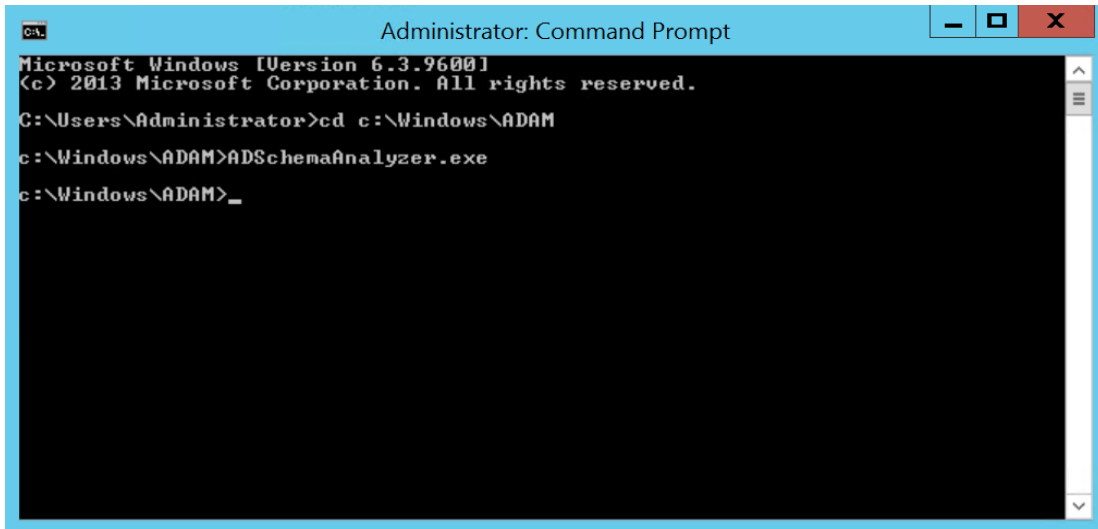


- 15) The AD LDS Instance is created showing the System Services under the Summary section.

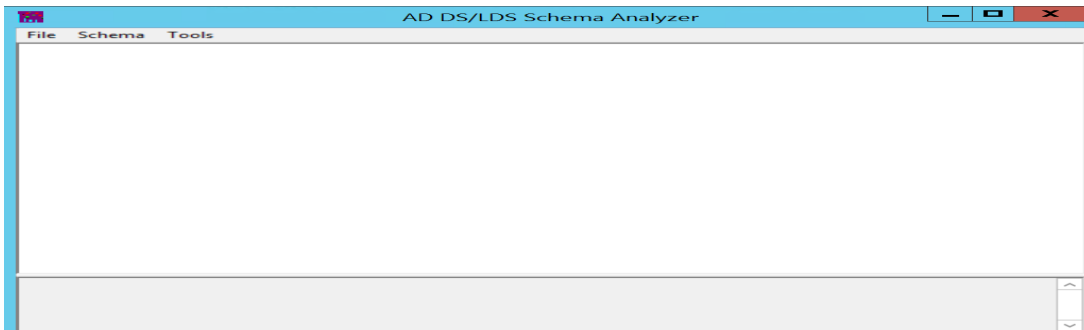


## Creating the Custom LDF File to suit for AD LDS Setup

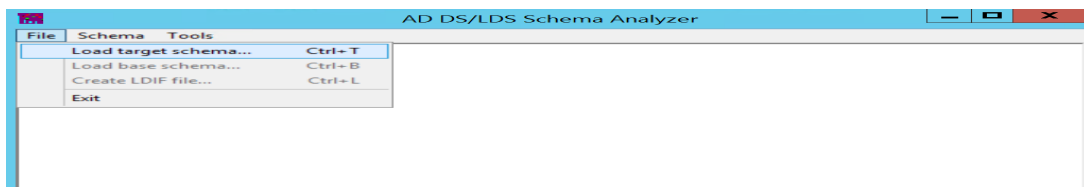
- 1) Open **Command Prompt** and then Go to C:\Windows\ADAM.



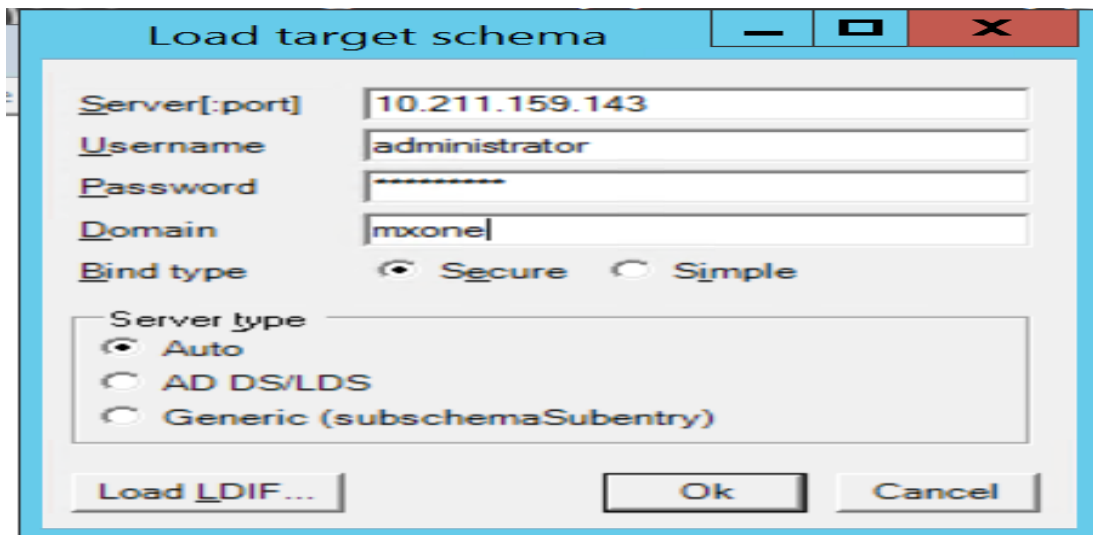
- 2) Execute ADSchemaAnalyzer.exe that displays a new window **AD DS / LDS Schema Analyzer**.



- 3) In **Schema Analyzer** window, go to **File** Menu and then select **Load Target Schema**.

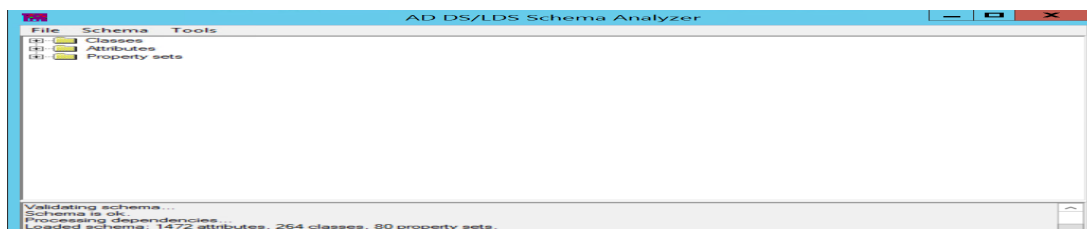


- 4) In **Load Target Schema** dialog box, provide the following details:
  - a) **Server[:port]:** [Give IP address of Active Directory Server]:[Active Directory port]
  - b) **Username:** [Username to connect to Active Directory]
  - c) **Password:** [Password of above username of Active Directory]
  - d) **Domain:** [Domain of Active Directory which contains above user]



**NOTE:** If you do not provide port number after server IP/DNS Name, it takes default LDAP port that is 389.

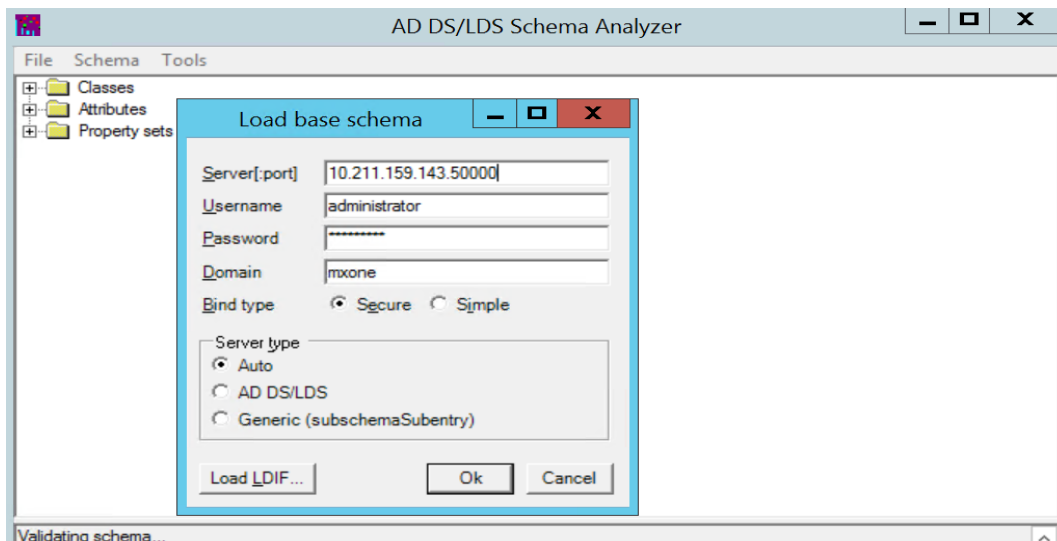
- 5) Click **Ok**.
- 6) **AD DS/LDS Schema Analyzer** screen shows the following folder structure. Once it is connected to Active Directory Server.



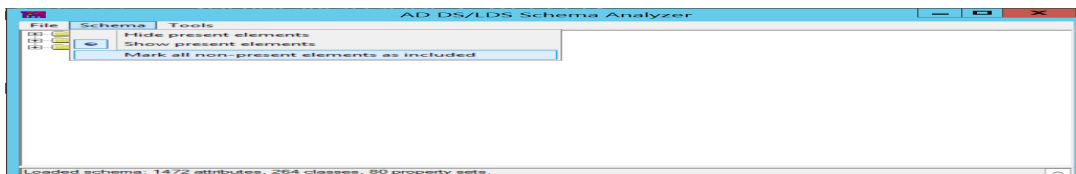
- 7) Go to **File** Menu and then select **Load base schema**.



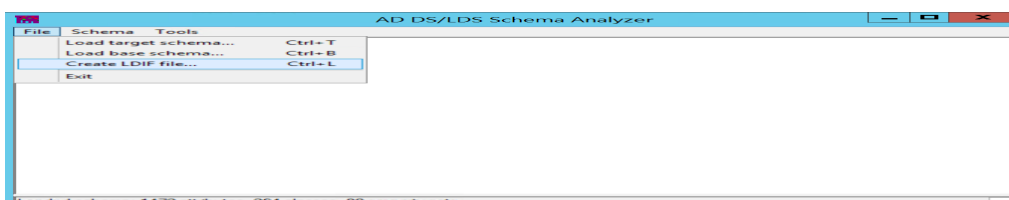
- 8) The **Load base schema** dialog box appears to enter the following details:
  - a) **Server[:Port]:** [Give IP address of AD LDS]:[AD LDS port]
  - b) **Username:** [Administrator Username of the local server]
  - c) **Password:** [Password of Administrator]
  - d) **Domain:** [Domain of Active Directory which contains above user]



- 9) Click **Ok**.
- 10) Go to **Schema** Menu and then select **Mark all non-present elements as included**.



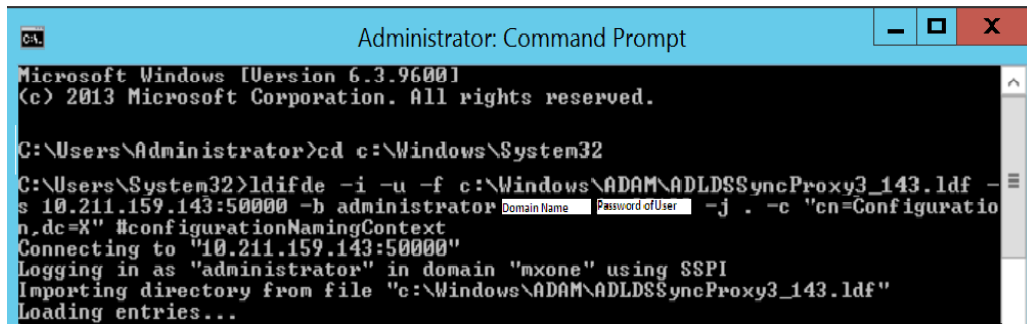
- 11) Click **Ok**.
- 12) Go to **File** Menu and then select **Create LDIF file**.



- 13) In the File Dialog box provide the path of LDIF file to store.
- 14) By default, it shows C:\Windows\ADAM Path.
- 15) Enter name of the file and click **Save**.
- 16) Open Command Prompt and then Go to C:\Windows\System32.
- 17) Execute the following 3 commands as mentioned below:
  - `ldifde -i -u -f [Path of LDIF File which is created by using Schema Analyzer] -s [IP address of AD LDS]:[Port of AD LDS] -b [Administrator Username of the local server] [Domain of Active Directory which contains above user] [Password of Administrator] -j . -c "cn=Configuration,dc=X" #configurationNamingContext`

*For example,*

```
ldifde -i -u -f c:\windows\adam\ADLDSSyncProxy3_129.ldf -s
192.168.26.129:50000 -b administrator pmsnmdomain XXXXXXXXXXXXXXXX -
j . -c "cn=Configuration,dc=X" #configurationNamingContext
```

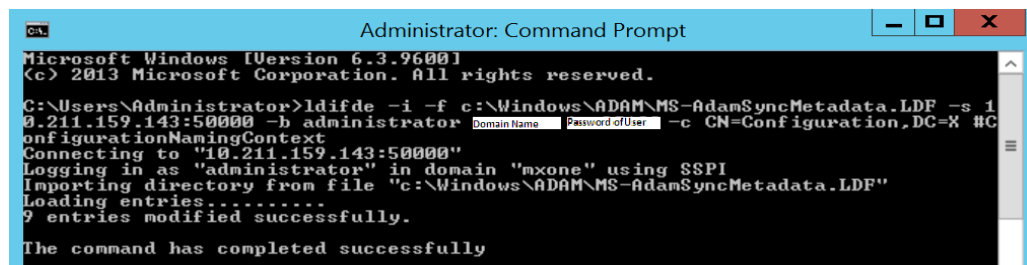


```
Administrator: Command Prompt
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>cd c:\Windows\System32
C:\Users\System32>ldifde -i -u -f c:\Windows\ADAM\ADLDSSyncProxy3_143.ldf -s
10.211.159.143:50000 -b administrator [Domain Name] [Password of User] -j . -c "cn=Configuratio
n,dc=X" #configurationNamingContext
Connecting to "10.211.159.143:50000"
Logging in as "administrator" in domain "mxone" using SSPI
Importing directory from file "c:\Windows\ADAM\ADLDSSyncProxy3_143.ldf"
Loading entries...
```

- `ldifde -i -f c:\windows\adam\MS-AdamSyncMetadata.ldf -s [IP address of AD LDS]:[Port of AD LDS] -b [Administrator Username of the local server] [Domain of Active Directory which contains above user] [Password of Administrator] -c CN=Configuration,DC=X #ConfigurationNamingContext`

*For example,* `ldifde -i -f c:\windows\adam\MS-AdamSyncMetadata.ldf -s 192.168.26.129:50000 -b administrator pmsnmdomain XXXXXXXXXXXXXXXX -c CN=Configuration,DC=X #ConfigurationNamingContext`



```
Administrator: Command Prompt
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ldifde -i -f c:\Windows\ADAM\MS-AdamSyncMetadata.LDF -s 1
0.211.159.143:50000 -b administrator [Domain Name] [Password of User] -c CN=Configuration,DC=X #C
onfigurationNamingContext
Connecting to "10.211.159.143:50000"
Logging in as "administrator" in domain "mxone" using SSPI
Importing directory from file "c:\Windows\ADAM\MS-AdamSyncMetadata.LDF"
Loading entries.....
9 entries modified successfully.

The command has completed successfully
```

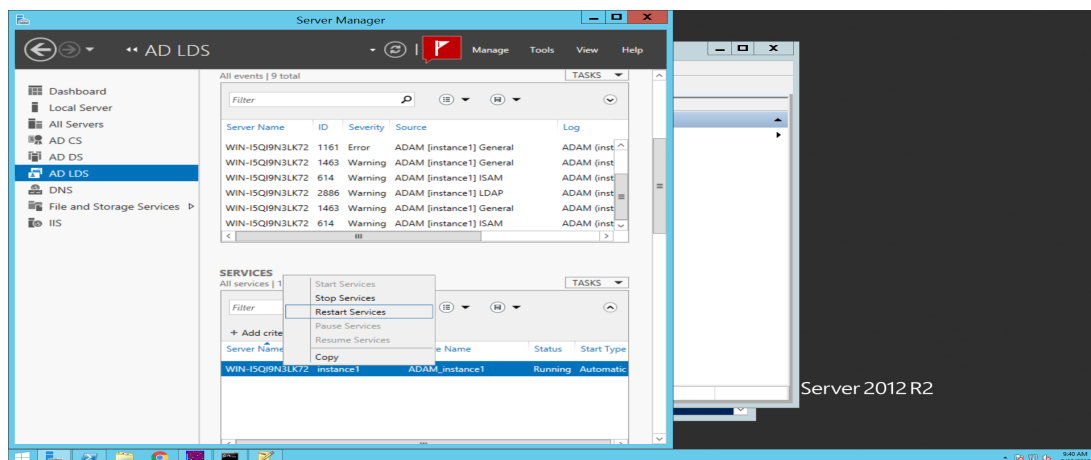
- `ldifde -i -f c:\windows\adam\MS-adamschemaw2k8.ldf -s [IP address of AD LDS]:[Port of AD LDS] -b [Administrator Username of the local server] [Domain of Active Directory which contains above user] [Password of Administrator] -c CN=Configuration,DC=X#ConfigurationNamingContext`

*For example,* `ldifde -i -f c:\windows\adam\MS-adamschemaw2k8.ldf -s 192.168.26.129:50000 -b administrator pmsnmdomain XXXXXXXXXXXXXXXX -c CN=Configuration,DC=X#ConfigurationNamingContext`

[illegible]

## Restarting the AD LDS Instance

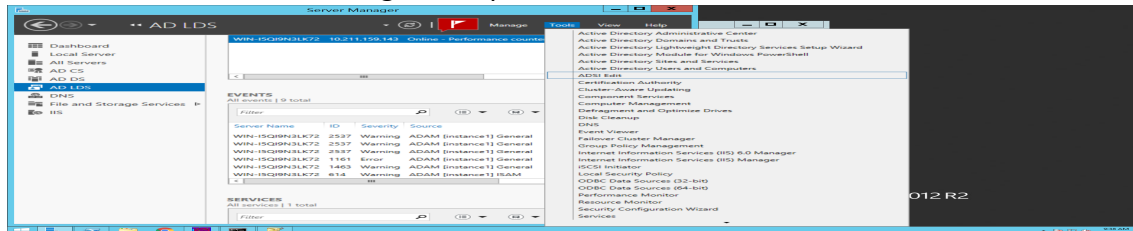
- 1) Select **Server Manager > Roles > Active Directory Lightweight Directory Services**.
- 2) Check for **System Services** section that is displayed in the right side pane.



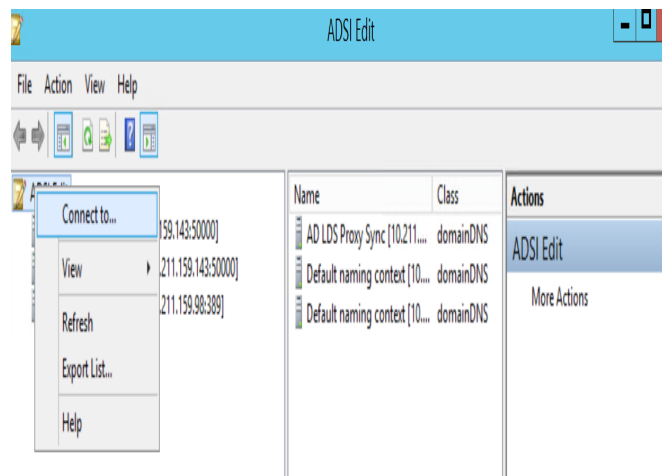
- 3) Select the AD LDS Instance Name and right click on the AD LDS instance, select **Restart/Stop – Start**.

## Creating an Admin User in AD LDS

- 1) Select Server Manager > Roles > Active Directory Lightweight Directory Services.
- 2) Select ADSI Edit shown in the right side pane, under the Advance Tools section.

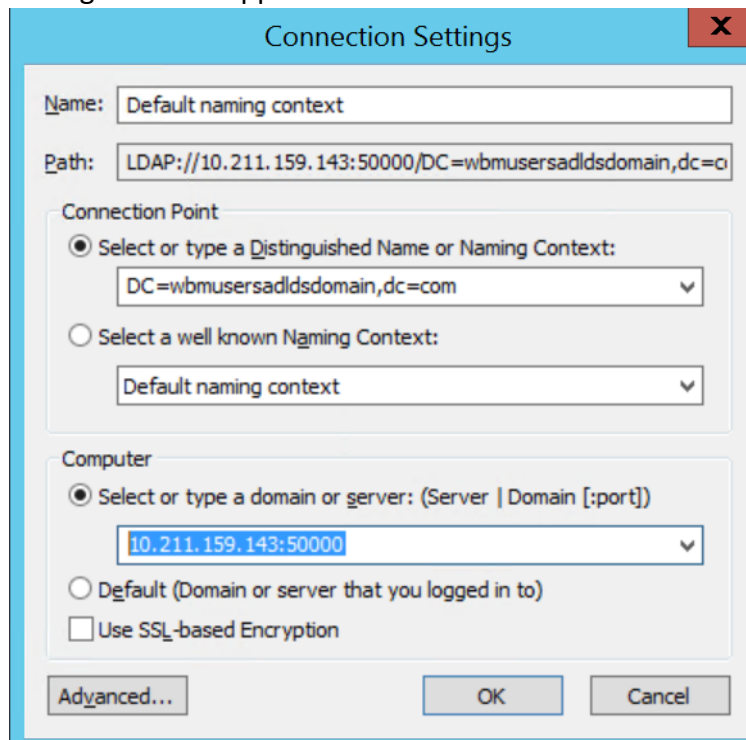


- 3) In ADSI Edit window, go to Action Menu, select Connect to... option, or right click on ADSI Edit in the left side pane.

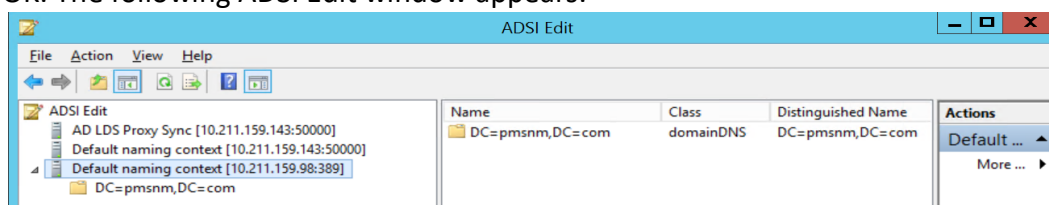




- 4) The Connection Settings window appears to fill the below details.

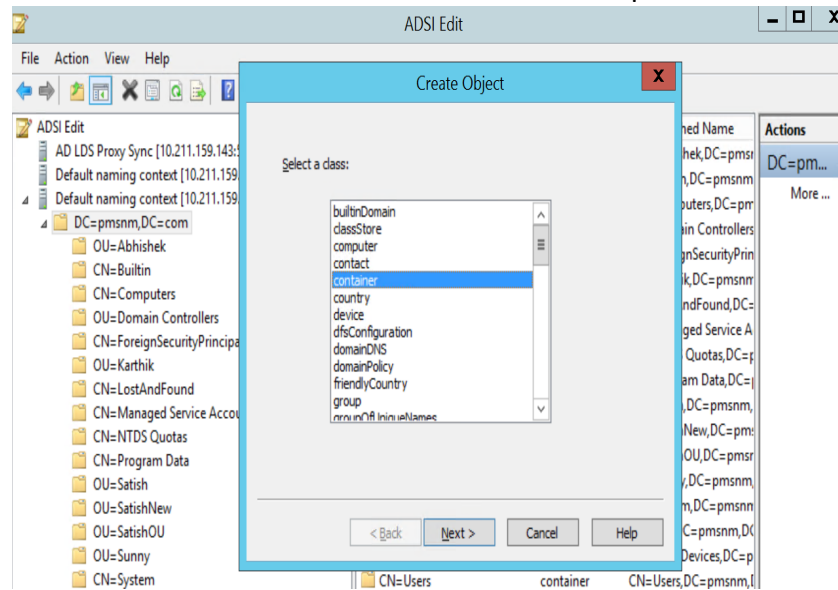


- 5) Enter Name to identify this AD LDS Instance.  
 6) In the Connection Point section, Select or type Distinguished Name or Naming Context and enter the Partition Name in AD LDS instance.  
 7) In the Computer section, Select or type a domain or server: (Server | Domain[:Port]) and enter the server IP of AD LDS and port details.  
 8) Click OK. The following ADSI Edit window appears.

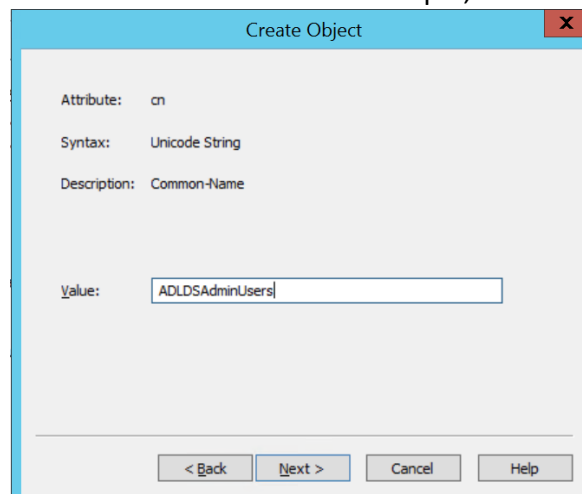


- 9) Right click on Partition/ Distinguished Name > select New > Object.  
 10) In ADSI Edit window, you can expand the right side pane to check Name and Distinguished Name.

- 11) In Create Object window > select container from the class list provided below.

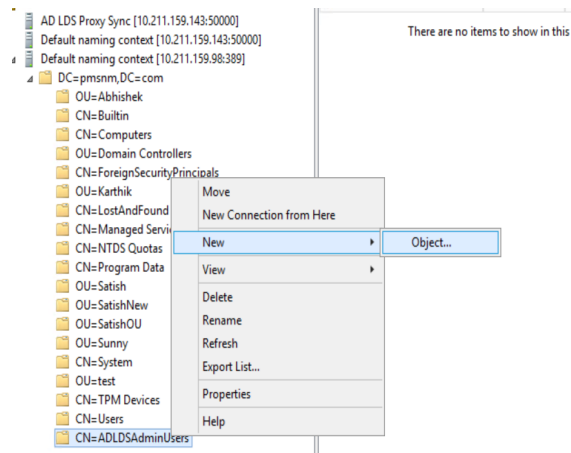


- 12) Click Next. The Create Object window appears to add value.
- 13) Enter name of the container in the Value box. For example, ADLDSAdminUsers and click Next.

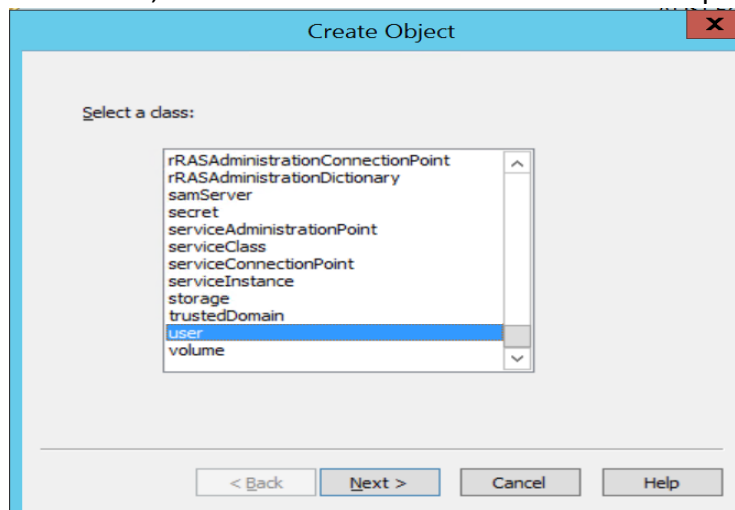


- 14) Click Finish.

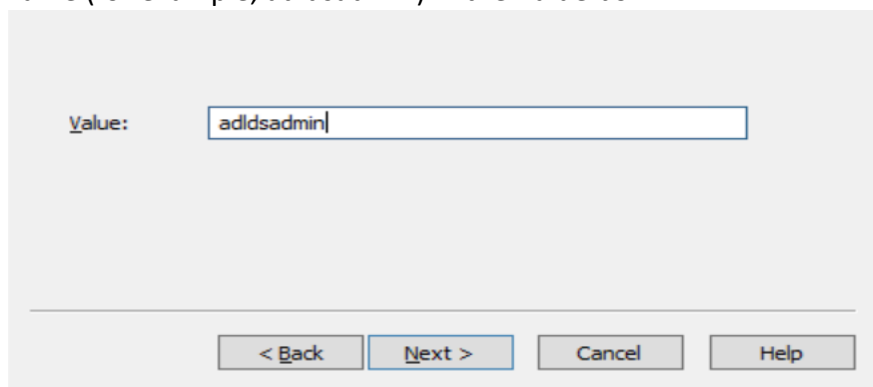
- 15) Right-click on the newly created container which is added under the Partition Name and select New > Object.



- 16) In the Create Object window, select user from the list of Class items displayed. Click Next.

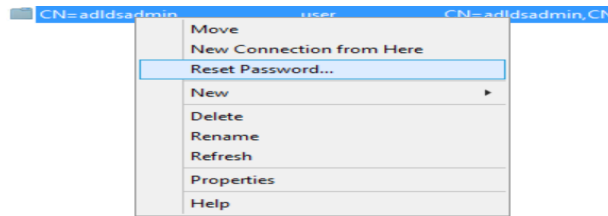


- 17) Enter a username (for example, adldsadmin) in the Value box.

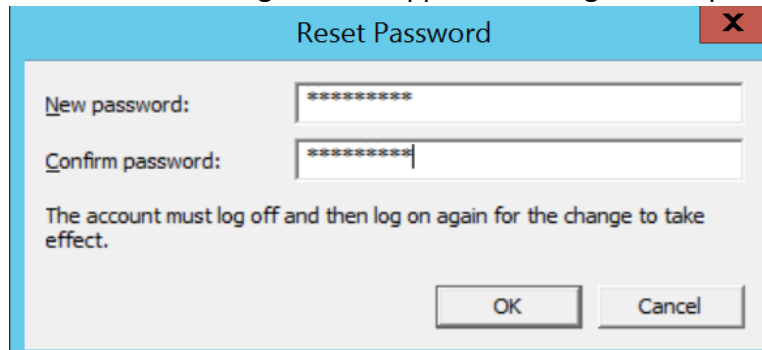


- 18) Click Next ? click Finish.

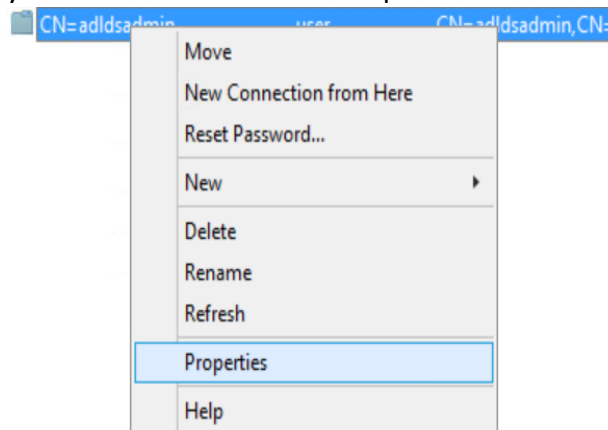
- 19) Expand newly created container and right click on the newly created user. The following window appears to Reset Password.



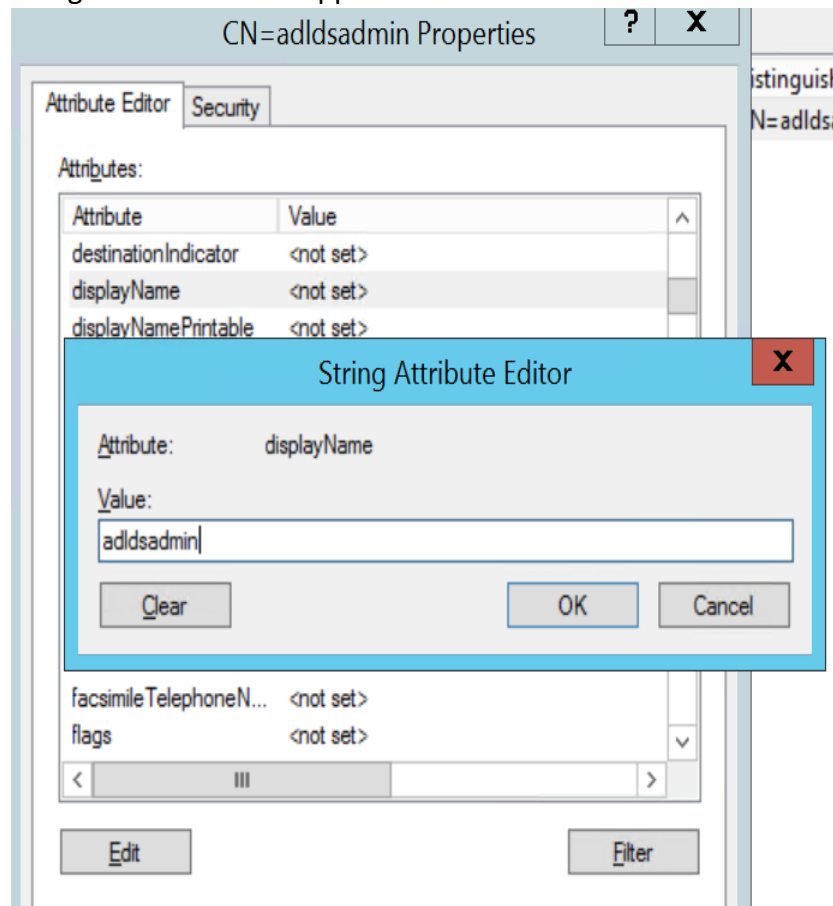
- 20) Select Reset Password. The following window appears to assign a new password for user.



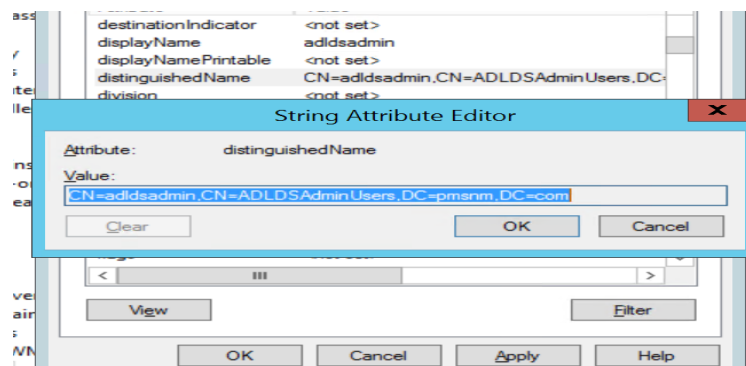
- 21) Enter the New password and Confirm password. Click OK.  
22) Right click on the newly created user and select Properties.



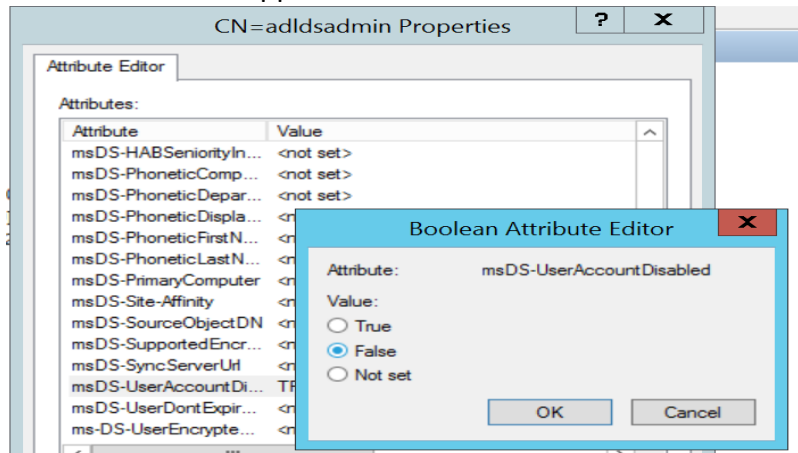
- 23) Right click on the newly created user properties dialog, select displayName and double click on it. The following String Attribute Editor appears.



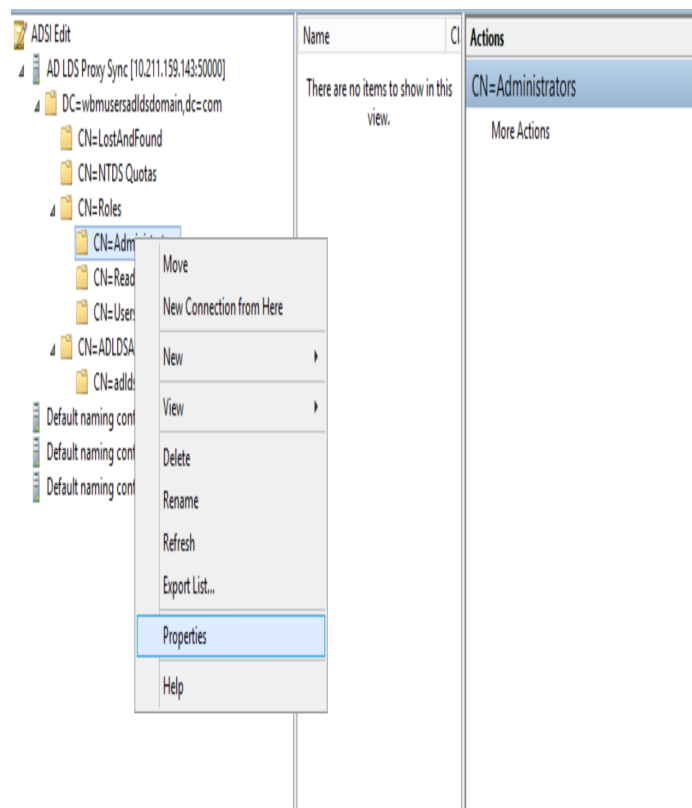
- 24) Enter the same username while resetting the password.  
25) Select distinguishedName ? double click on it to copy the distinguishedName value.  
26) Click OK.



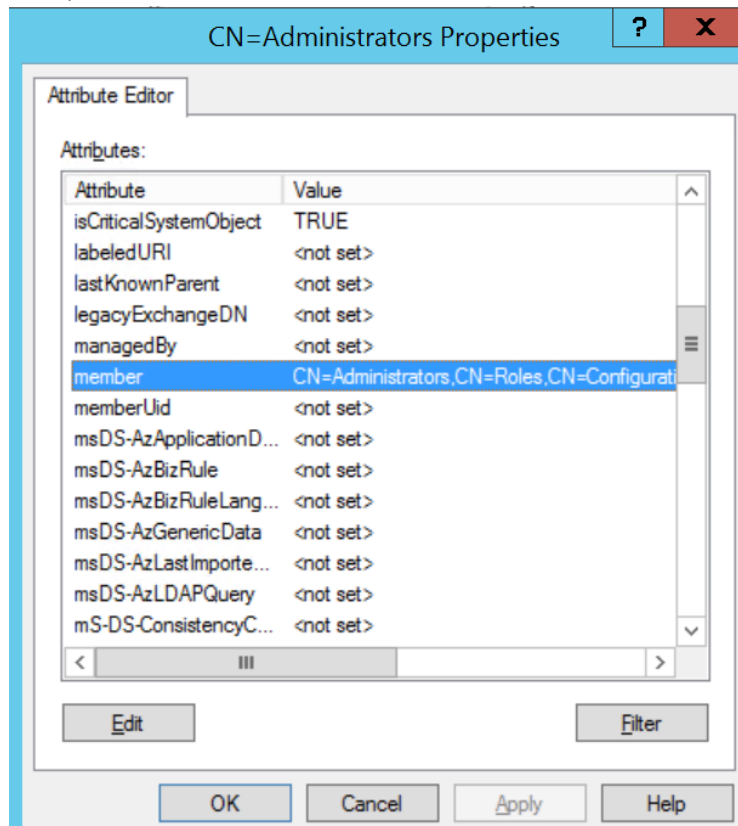
- 27) In the same attribute editor Select msDS-UserAccountDisabled and double click on it. The following Boolean Attribute Editor window appears.



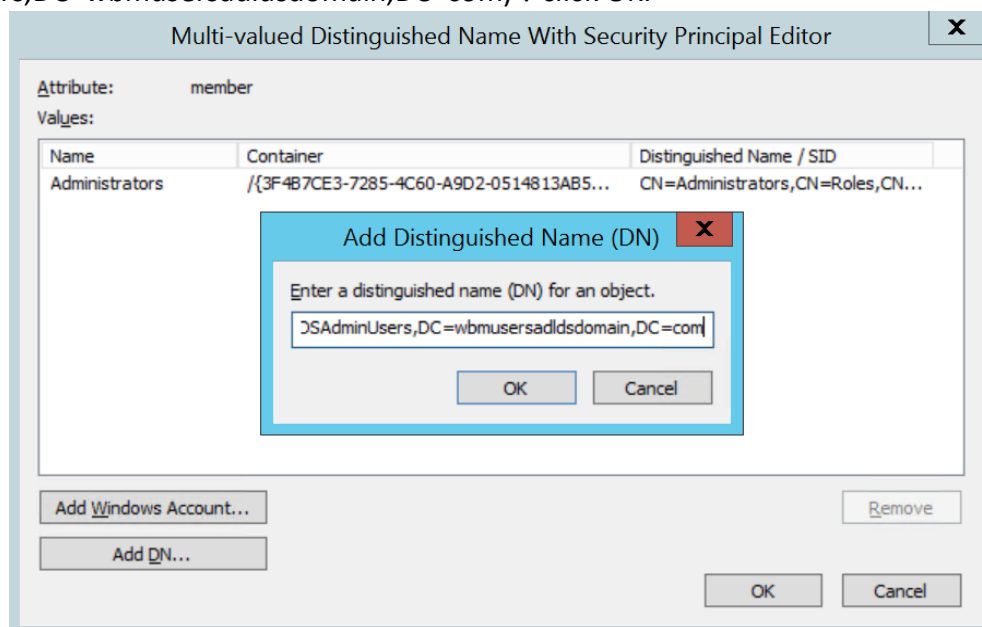
- 28) Select False and click OK.  
 29) Click Apply > OK.  
 30) Expand the newly created partition name and CN=Roles. Right click on CN=Administrators?Properties to view the Attribute Editor.



- 31) In the Attribute Editor, select member and click Edit.



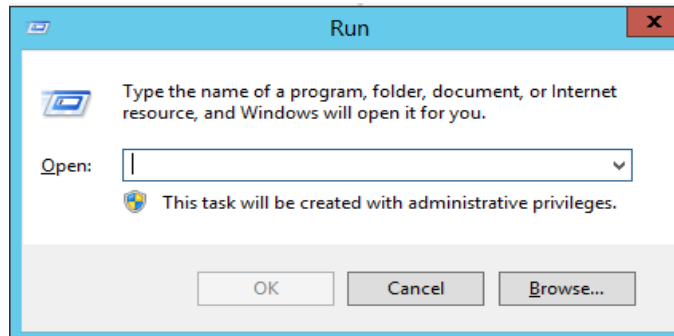
- 32) Click Add DN button > Enter DN of user created above (for example, CN=adldsadmin,CN=ADLDSAdminUsers,DC=wbmusersadldsdomain,DC=com) ? click OK.



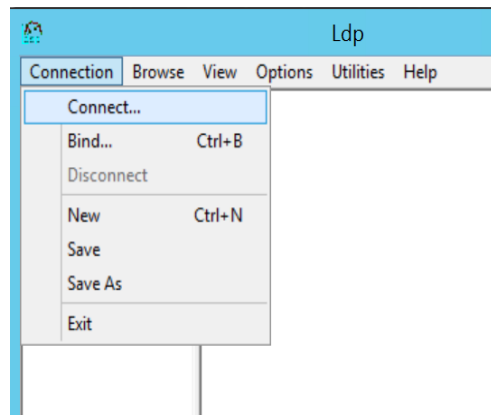
- 33) Click OK > click Apply > click OK.

## Checking User Authentication

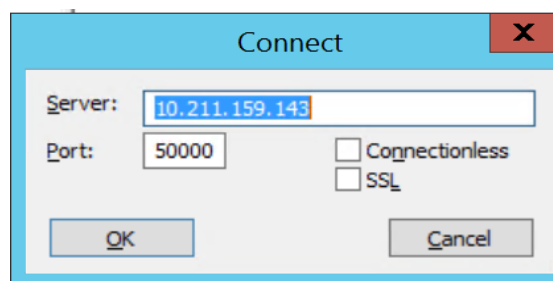
- 1) On the **Start** Menu, click **Run**. The following **Run** program window appears.



- 2) Type **ldp.exe** (**Label Distribution Protocol**) in the **Run** box and click **OK** to open **Ldp.exe** window.
- 3) In **LDP** window, Go to **Connection** and click **Connect**.

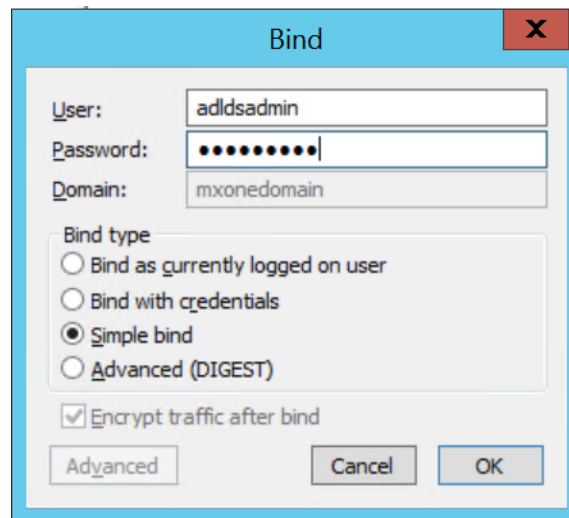


- 4) Enter the IP **Server** address and **Port** number of AD LDS Instance and click **OK**.



- 5) Go to **Connection** and click **Bind**. The following Bind window appears.





- 6) To connect and bind the server that hosts the forest root domain of your AD DS environment. Enter the following details:
- User:** [username which is created above]
  - Password:** [Password of the above user]
  - Domain:** By default, remains in deactivate mode
  - Bind Type:** [select Simple bind]
  - Click **OK**.
- NOTE:** The user must be an authenticated user as mentioned in the above screen.*
- An example of successful authentication is given below.

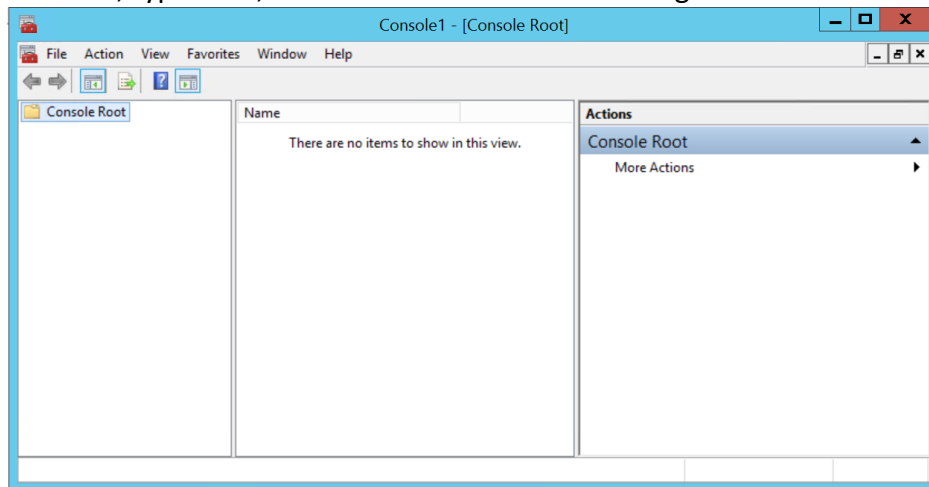
```

-----
res = ldap_simple_bind_s(ld, 'adldsadmin', <unavailable>); // v.3
Authenticated as: 'CN=adldsadmin,CN=ADLDSAdminUsers,DC=wbmusersadldsdomain,DC=com'.
-----
|

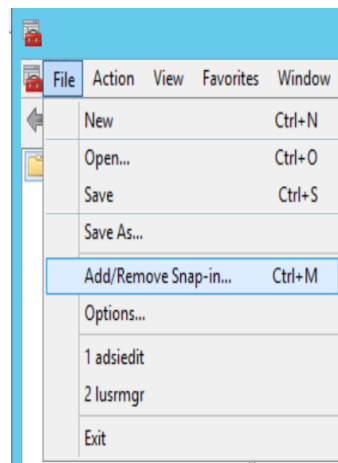
```

## Adding Attributes to UserProxyFull Class

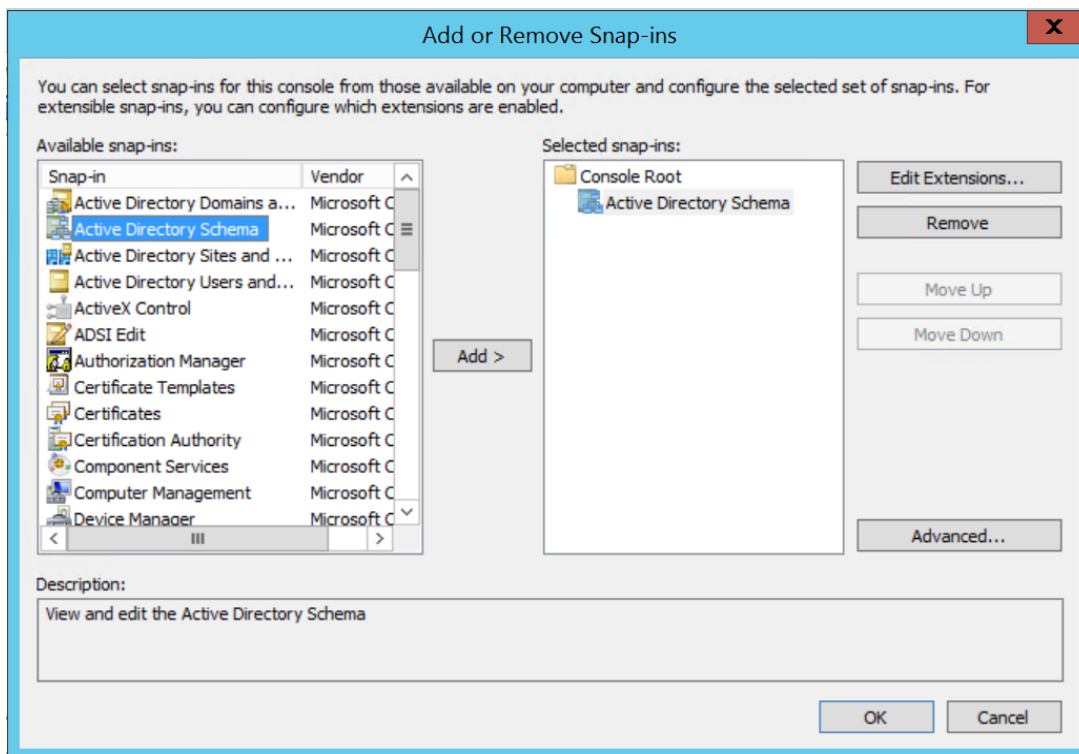
- 1) On the **Start** Menu, type **FMC**, and then click **OK**. The following **Console** window appears.



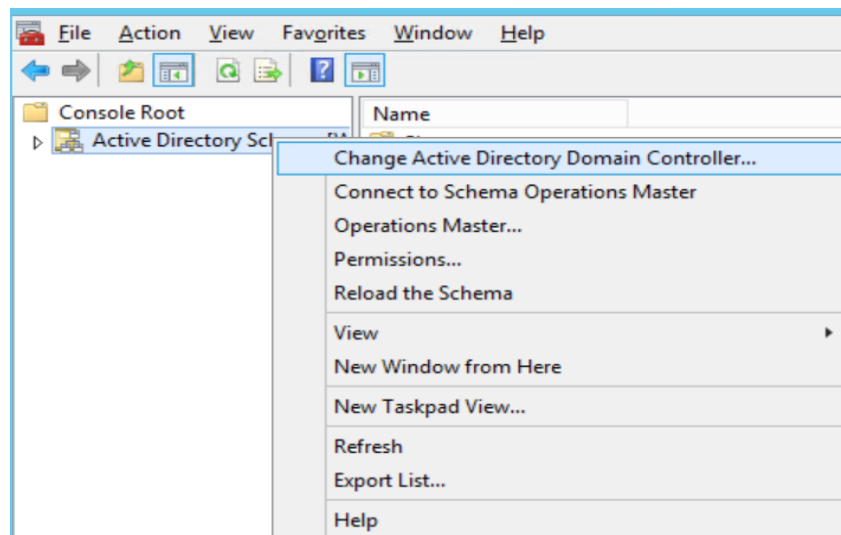
- 2) Go to **File** menu > click **Add/Remove Snap-in**.



- 3) Select **Active Directory Schema**, click **Add** and then click **OK**.



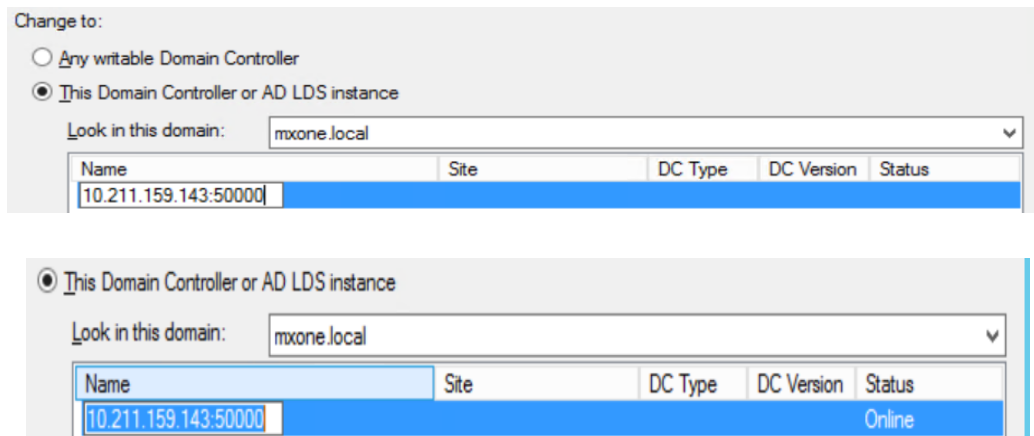
- 4) Right click on **Active Directory Schema** and select **Change Active Directory Domain Controller**.



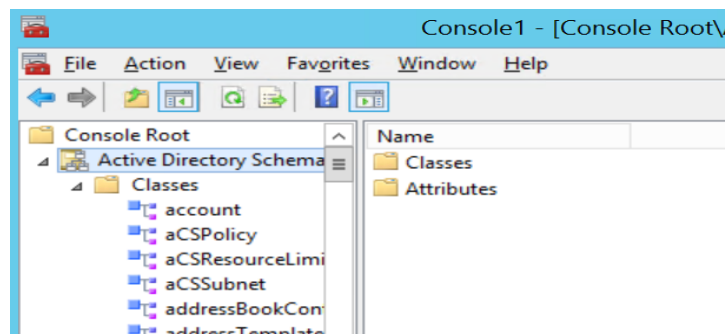
- 5) Select **This Domain Controller or AD LDS instance**.



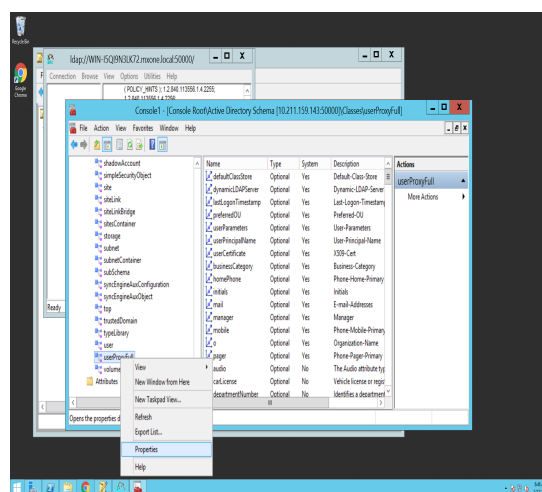
- 6) Enter IP Address of the **AD LDS Instance** with port number and click outside of the highlighted edit area. The **Status** column value changes to **Online**.



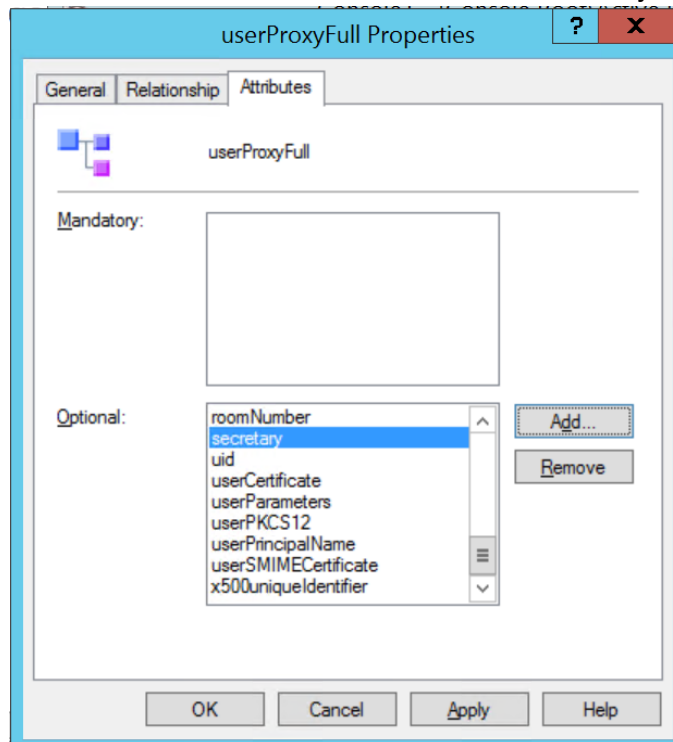
- 7) Select this entry (that is, anywhere outside from the edit section) > click **OK** > click **Yes**.
- 8) Expand **Classes** to select the required attributes displayed in the **Classes** list.



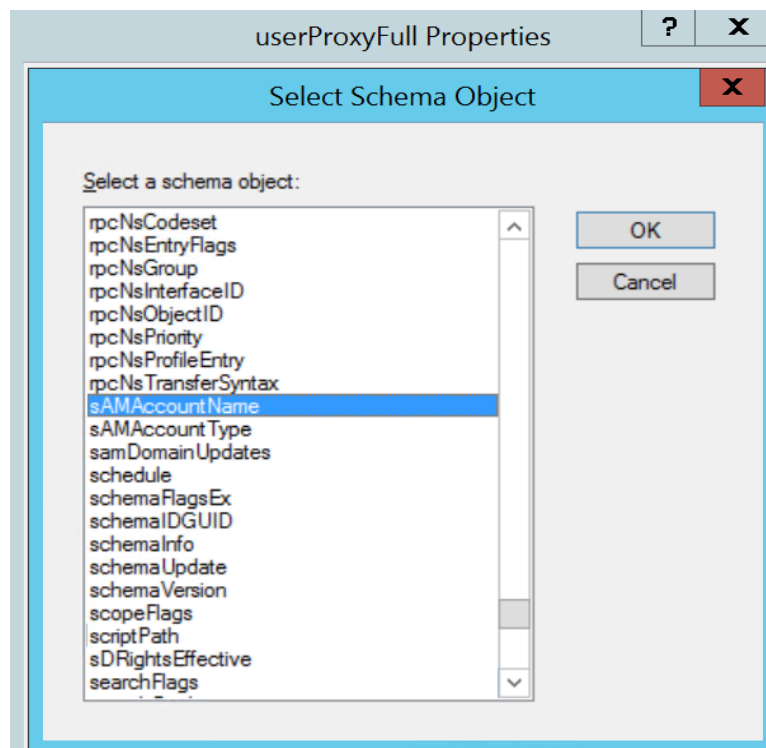
- 9) Select **userProxyFull** from the Classes list and right click on it to select **Properties**.



- 10) Go to **Attributes** tab and check for the **sAMAccountName** attribute. If **sAMAccountName** attribute is not available, then click **Add** button to include it to the Schema Object list.



- 11) Select **sAMAccountName** > click **OK** > click **Apply** > click **OK**.



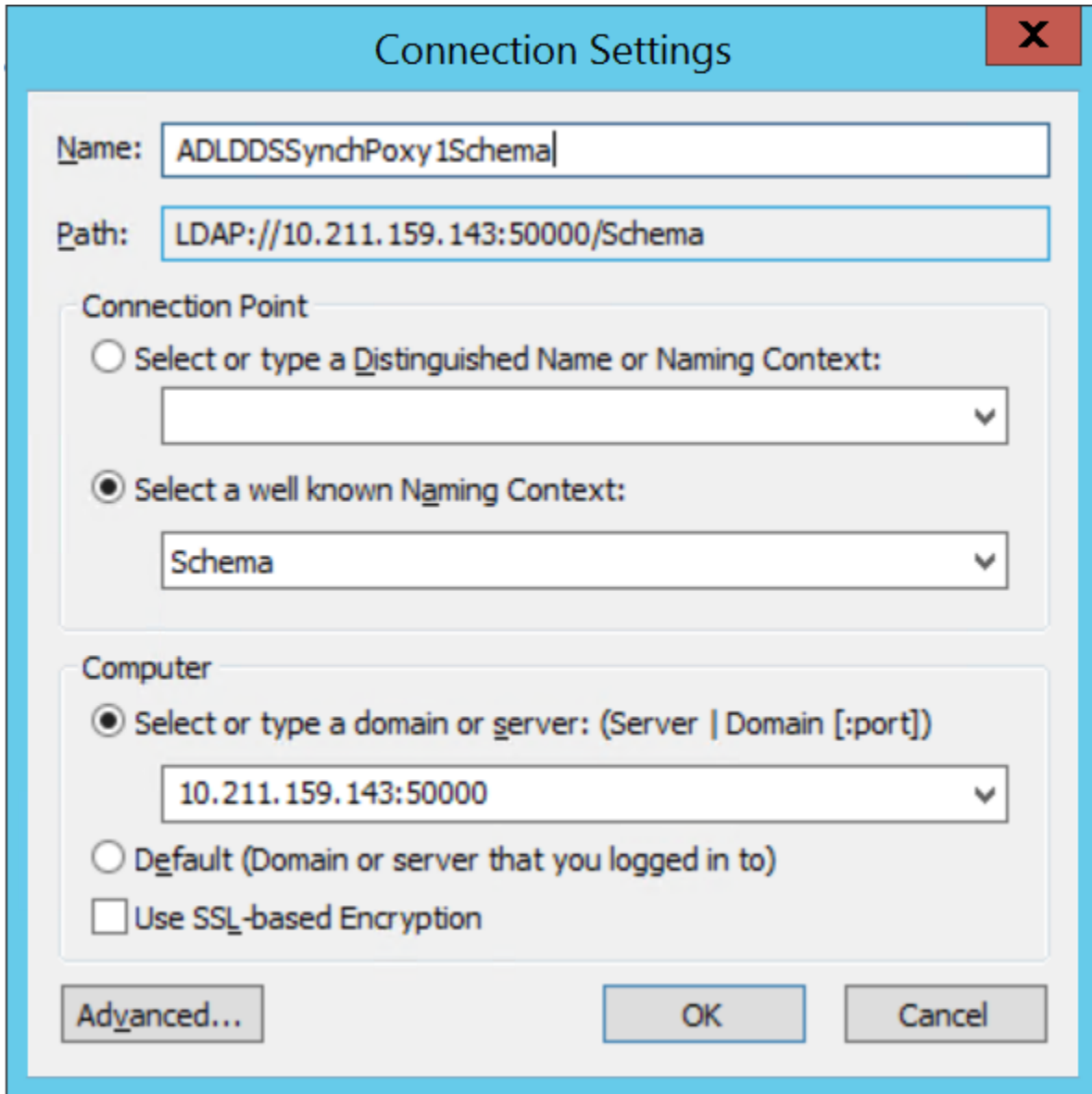
*In the same way, you can check and add the below attributes:*

- objectSID
- sn
- department
- location
- whenChanged
- telephoneNumber
- wWWHomePage
- description
- physicalDeliveryOfficeName
- url
- streetAddress
- postOfficeBox
- l[Locality-Name]
- st
- postalCode
- c[Country-Name]
- profilePath
- scriptPath
- title
- company
- facsimileTelephoneNumber
- otherFacsimileTelephoneNumber
- msExchAssistantName
- roomNumber
- ipPhone
- objectClass
- objectCategory
- lastAgedChange

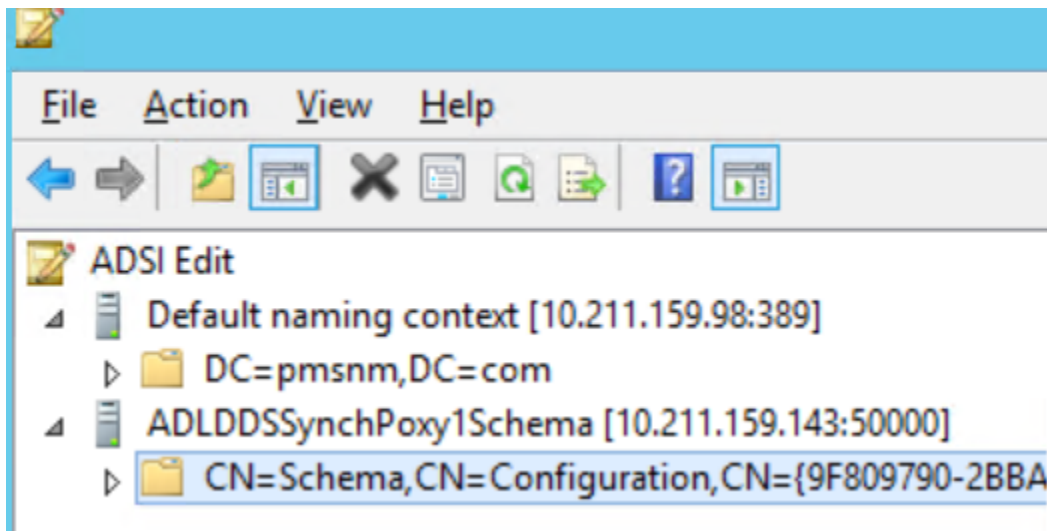
12) Restart AD LDS Instance when all the required attributes are added and checked.

## Editing Object (UserProxyFull) Class as User Object Class

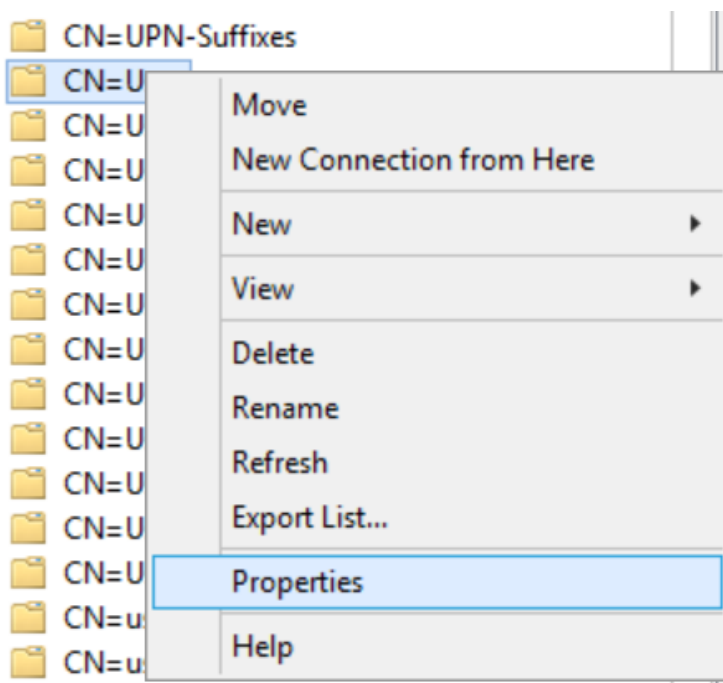
- 1) In the **ADSI Edit** Console tree, click **ADSI Edit** node and then click the **Action** menu. Select **Connect to**. The **Connection Settings** dialog box appears.



- 2) In **Connection Point** section, click **Select a well known Naming Context** radio button.
- 3) In **Computer** section, select or type a domain or server: (Server | Domain [:port]) of AD LDS Instance.
- 4) Select **Schema** from the drop-down list.
- 5) Expand **Schema** from left side pane > expand CN=Schema, CN=Configuration, CN={XXXXXXXX}.

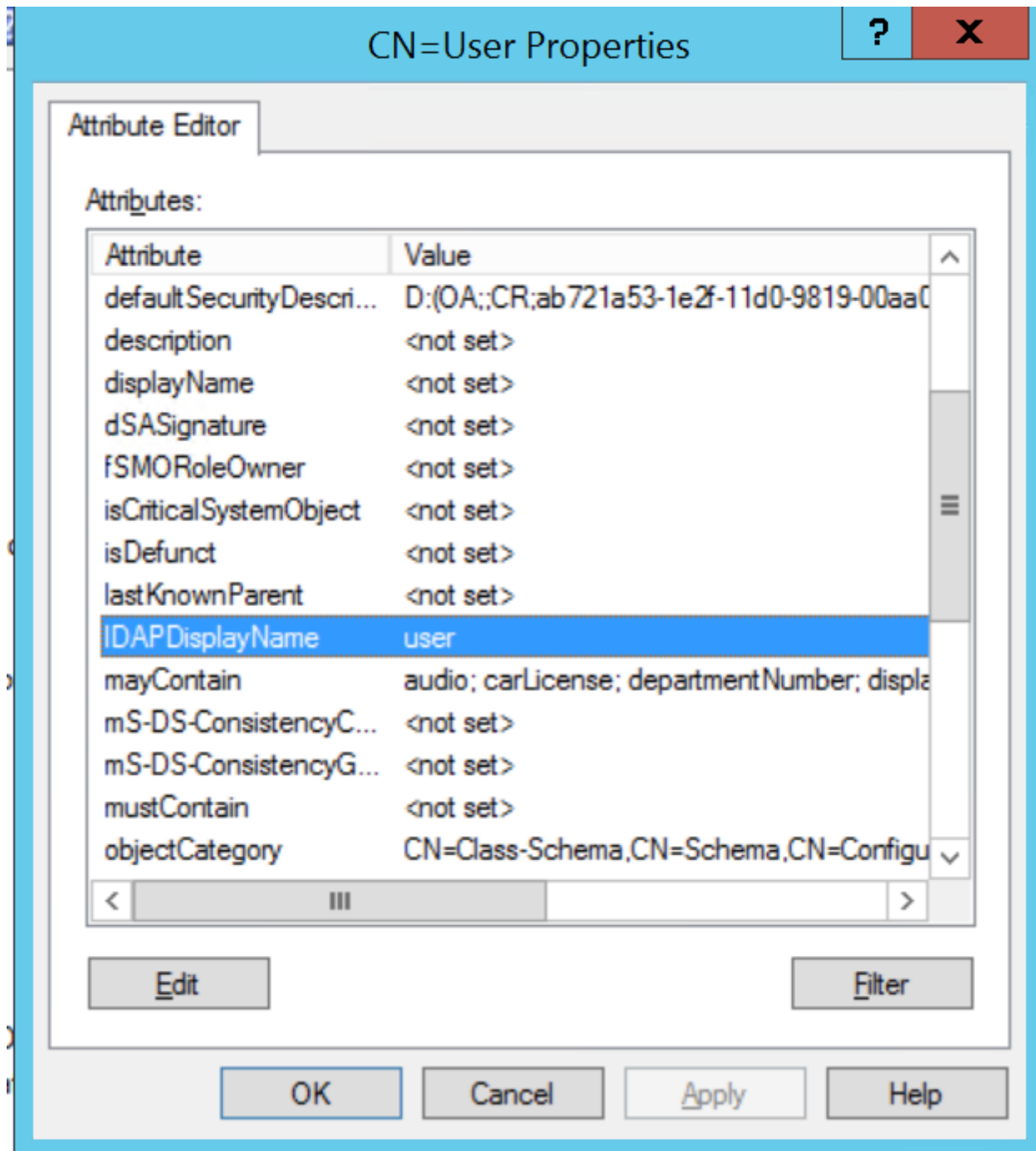


- 6) Select **CN=User**, and then right-click on it and select **Properties**.

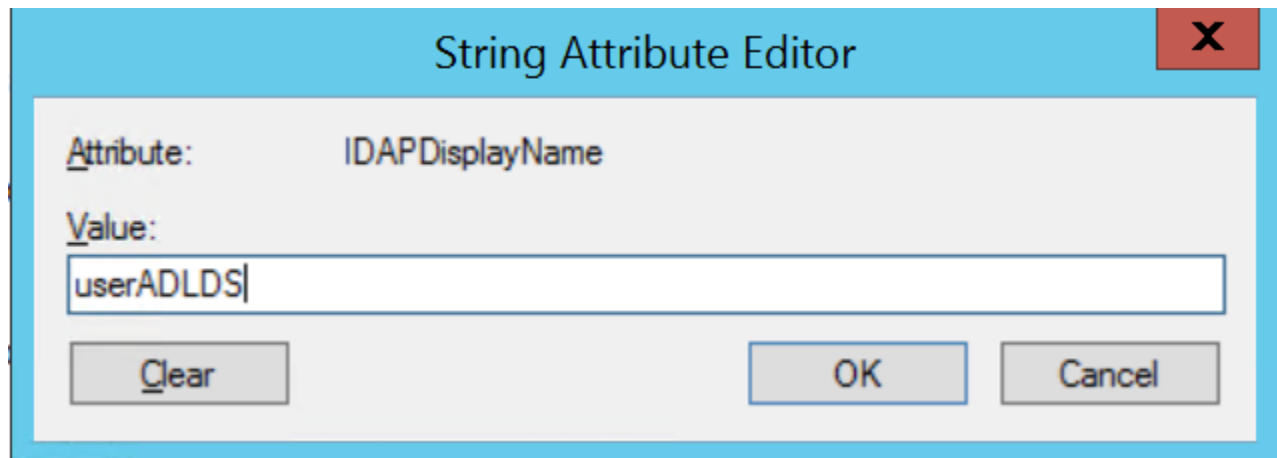


- 7) Select **IDAPDisplayName** and double click on it to modify the selected attribute value.

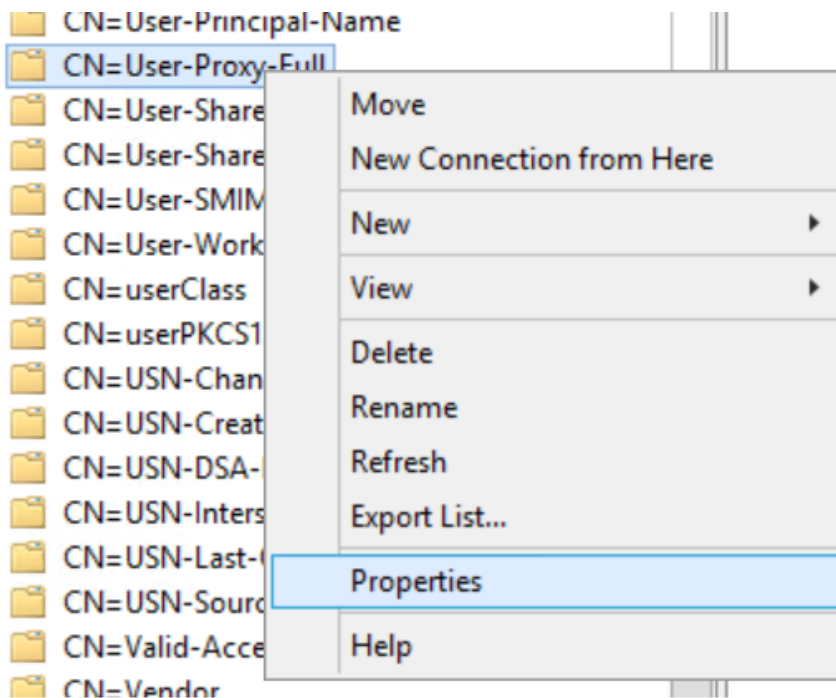




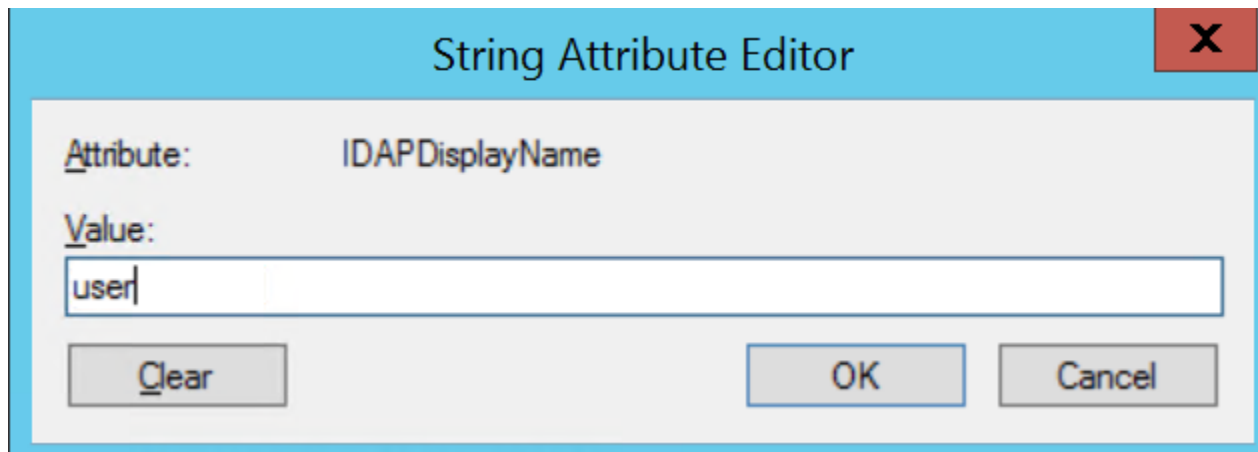
- 8) Change value to **userADLDS** (this is just a dummy name), then click **Apply**, and click **OK**.



- 9) In the same way, you can change the **IDAPDisplayName** value of **user-Proxy-Full** to user. Once the changed attribute value is applied, you must restart **AD LDS Instance**.



- 10) Change it to **user**. Click **OK**. Click **Apply** and then click **OK**.



## Modifying MS-AdamSyncConf File

- 1) Go to C:\Windows\ADAM Directory in windows. Copy and Paste *MS-AdamSyncConf.xml* file. Rename the newly created file (for example, *MS-AdamSyncConf\_Document.xml*).

This PC	ADLDSyncProxy_143	2/13/2019 6:14 AM	LDF File	1,895 KB
Desktop	ldif.err	2/13/2019 6:09 AM	ERR File	1 KB
Documents	LDF file	2/12/2019 6:25 AM	LDF File	2 KB
Downloads	WBMSync	2/6/2019 2:15 PM	Text Document	2 KB
Music	MS-AdamSyncConf_Doc	1/8/2019 2:27 PM	XML Document	3 KB
Pictures	MS-AdamSyncConf1	1/8/2019 2:26 PM	Text Document	3 KB
Videos	ADLDSyncProxy5_143	1/8/2019 1:20 PM	LDF File	3 KB
Local Disk (C:)	adammsg.dll	1/8/2019 7:30 AM	Application extens...	4 KB
	adamntds.dit	1/8/2019 7:30 AM	DIT File	4,112 KB

- 2) Open the file in Edit mode (using Notepad) and modify below fields.  
`<source-ad-name>Domain Name of Active Directory</source-ad-name>`  
`<source-ad-partition>Partition Name of Active Directory</source-ad-partition>`  
`<source-ad-account>[user name of Active Directory Admin]</source-ad-account>`  
`<account-domain>[Above Username Account Domain]</account-domain>`  
`<target-dn>[DN/Partition in AD LDS]</target-dn>`  
`<base-dn>[DN of users from which we want to synchronize from Active Directory]</base-dn>`

For Example:

```
<source-ad-name>pmsnmdomain.com</source-ad-name>
<source-ad-partition>dc=pmsnmdomain,dc=com</source-ad-partition>
<source-ad-account>administrator</source-ad-account>
<account-domain>pmsnmdomain</account-domain>
<target-dn>DC=wbmusersadldsdomain,dc=com</target-dn>
<base-dn>OU=WBMUSers,DC=pmsnmdomain,DC=com</base-dn>
```

- 3) Save the modified file.

## Synchronizing Users from Active Directory to AD LDS Instance

- 1) Open Command Prompt. Go to C:\Windows\ADAM.
- 2) Execute the following 2 commands as mentioned below.
  - a) `adamsync.exe /install [AD LDS Instance IP:Port] [MS-ADAMSync-Conf.xml File Name] /passprompt`  
*For example: `adamsync.exe /install 192.168.26.129:53986 MS-AdamSync-Conf_Docuent.xml /passprompt`*  
**NOTE:** To synchronize users from Active Directory to AD LDS Instance, you must run the Adam-sync.exe utility.  
Enter the password of Active Directory user which is mentioned in the XML file.

```
C:\Windows\ADAM>adamsync.exe /install 192.168.26.129:50000 MS-AdamSyncConf_Docum
ent.XML /passprompt
Please enter password:
Done.
C:\Windows\ADAM>_
```

- b) `adamsync.exe /sync [AD LDS Instance IP:Port] "[DN/Partition Name of AD LDS]" /log [Log File Name]`  
*For example: `adamsync.exe /sync 192.168.26.129:53986 "DC=wbmuser-sadldsdomain,dc=com" /log WBMSync.log`*

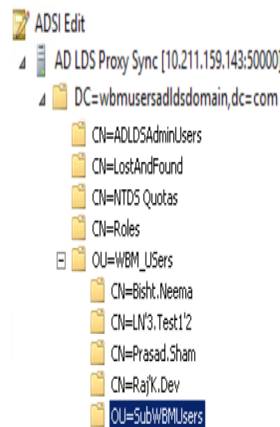
```
C:\Windows\ADAM>
C:\Windows\ADAM>
C:\Windows\ADAM>adamsync.exe /sync 192.168.26.129:50000 "DC=wbmusersadldsdomain,
dc=com" /log WBMSync.log
_
```

**NOTE:** WBMSync.log contains the user synchronization information from Active Directory to AD LDS. If any issues occurred while synchronization, it gets recorded in this log. All the users get synchronized from the Container to AD LDS except their passwords. So, you need to wait until the user synchronization process is completed.

## Checking Synchronized Users in AD LDS

- 1) Open **Server Manager** > expand **Roles** > select **Active Directory Lightweight Directory Services**.
- 2) In **Advanced Tools** section, select **ADSI Edit** that is displayed in the right side pane.
- 3) In **ADSI Edit** window, go to **Action** menu and select **Connect to**, then provide the below details.
- 4) In **Connection Point** section, click **Select or Type Distinguished Name or Naming Context** and enter **Partition Name**.
- 5) In **Computer** section, click **Select or type domain or server: (Server | Domain [:Port])** of AD LDS Instance.

- 6) (Enter the IP address of AD LDS server with port number, for example: 192.168.26.129:50000).



- 7) All the Active Directory Users of that particular container and sub-containers gets synchronized and visible under the **ADSI Edit** Console tree.

## Enabling LDAPS (SSL) for AD LDS in Window Server

- 1) Create a separate directory in the user location in the system.
- 2) Create a file *adlds\_request.inf* (file name can be anything with .inf extension).
- 3) Copy the below highlighted content in that file and change the required value in pink color.

**NOTE:** Remember that “;” is a comment in this file.

```
;----- request.inf -----[Version]
Signature="$Windows NT$"
[NewRequest]
Subject = "Fully Qualified name of AD LDS server" ; replace with the FQDN
of the DCKeySpec = 1KeyLength = bitsize can be any value from below line
values; Can be 1024, 2048, 4096, 8192, or 16384.; Larger key sizes are
more secure, but have; a greater impact on performance.Exportable =
TRUEMachineKeySet = TRUESMIME = FalsePrivateKeyArchive =
FALSEUserProtected = FALSEUseExistingKeySet = FALSEProviderName =
"Microsoft RSA SChannel Cryptographic Provider"ProviderType =
12RequestType = PKCS10KeyUsage =
0xa0[EnhancedKeyUsageExtension]OID=1.3.6.1.5.5.7.3.1 ; this is for Server
Authentication;-----
```

- 4) Execute the below command in directory to create a certificate request.certreq -new <.inf file name> <certificate request file name>

*An example of the command is mentioned below.*

```
c:\Certificates\ADLDS_Certs\ADLDS_Keystore_Dir>certreq -new Certificate_request_details.inf ADLDS_Request_file.req
c:\Certificates\ADLDS_Certs\ADLDS_Keystore_Dir>
```

- 5) A new file is created in the same directory.

```
c:\Certificates\ADLDS_Certs\ADLDS_Keystore_Dir>dir
Volume in drive C has no label.
Volume Serial Number is 3AC0-320A

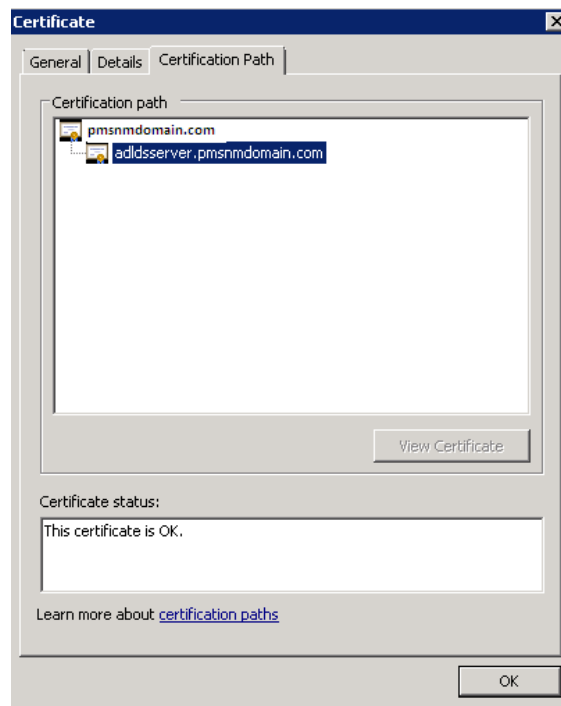
Directory of c:\Certificates\ADLDS_Certs\ADLDS_Keystore_Dir

11/11/2016  05:40 AM    <DIR>          .
11/11/2016  05:40 AM    <DIR>          ..
11/11/2016  05:40 AM                1,380 ADLDS_Request_file.req
11/11/2016  02:19 AM                763 Certificate_request_details.inf
                2 File(s)                2,143 bytes
                2 Dir(s)  6,052,823,040 bytes free

c:\Certificates\ADLDS_Certs\ADLDS_Keystore_Dir>
```

- 6) Share the file with Certificate Authority to provide the signed certificate.  
7) Copy the file in the same directory (with preferred extension of .cer / .crt).

*For example, the sample AD LDS Server Signed Certificate (in this **pmsnmdomain.com** is root certificate), which is certificate of Issuer who has issued certificate to AD LDS Instance. **Adldsserv-er.pmsnmdomain.com** – is the Signed Certificate of AD LDS Instance.*

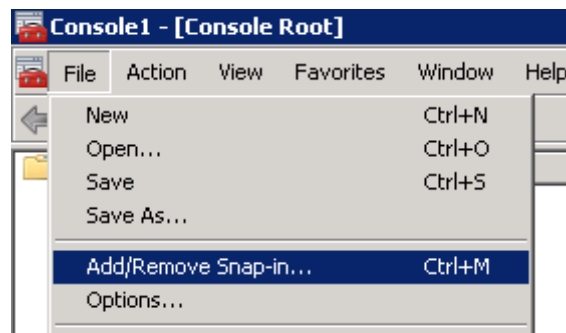


- 8) Once you receive the signed certificate from Certificate Authority. Type the below mentioned command. `certreq -accept <received signed certificate file name>`  
*An example of the command is mentioned below.*

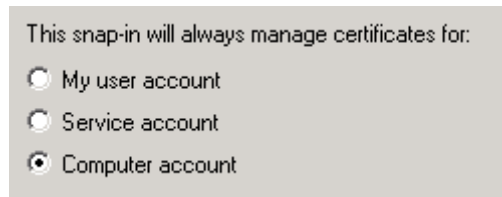
```
c:\Certificates\ADLDS_Certs\ADLDS_Keystore_Dir>certreq -accept ADLDS_Cert_Response.cer
c:\Certificates\ADLDS_Certs\ADLDS_Keystore_Dir>
```

- 9) Open **Command Prompt** and **Run as Administrator**.

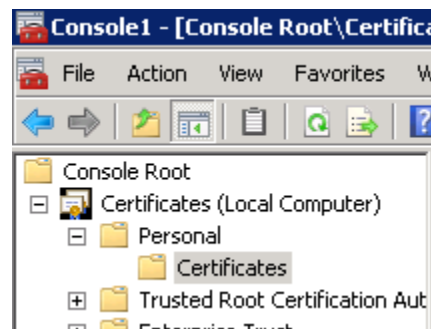
- 10) In the command prompt, execute *mmc* command that opens a new mmc window.
- 11) In the *mmc* window, go to **File** and select **Add/Remove Snap-in** option.



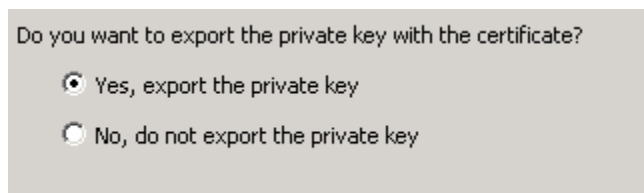
- 12) In the **Add or Remove Snap Ins** window, select **Certificates** from the left side pane and click on **Add** button.
- 13) Select **Computer Account** and click **Next**. Select **Local Computer**. Click **Finish** and then click **OK**.



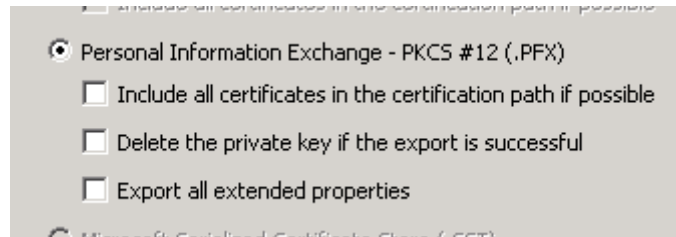
- 14) Extract **Certificates > Personal > Certificates** from the left side pane. All the certificates get listed in the right side pane.



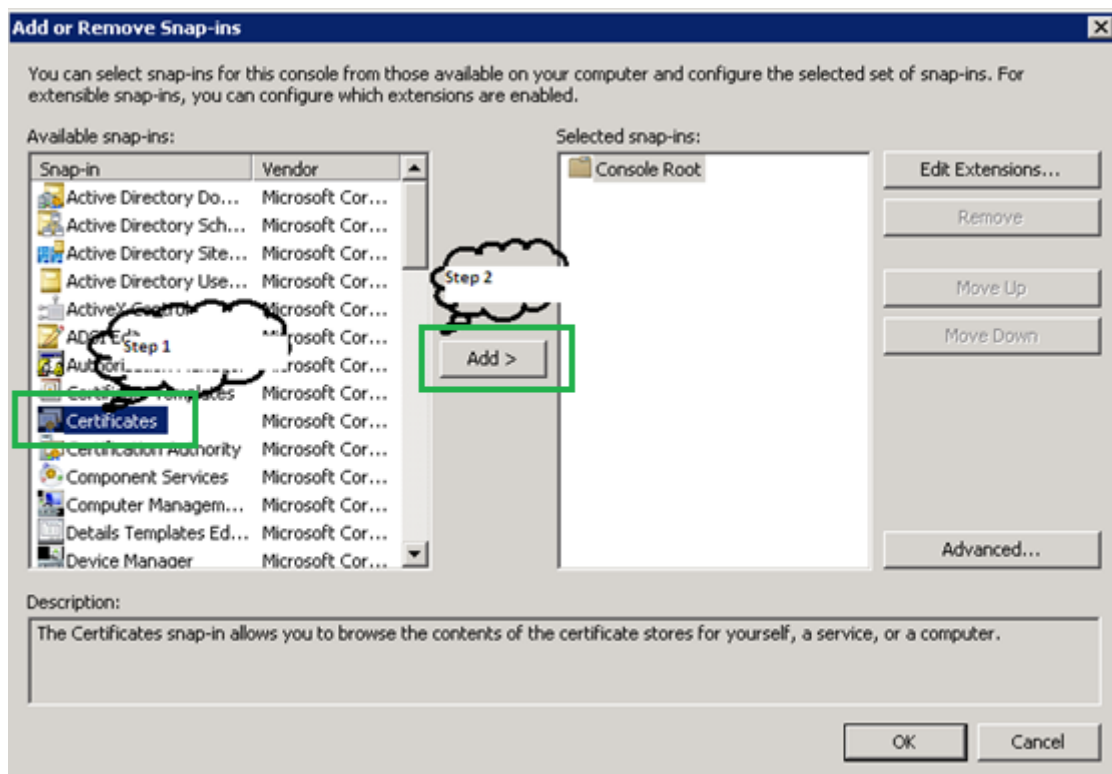
- 15) Open the Signed certificate which you have received from Certificate Authority.
- 16) Once the certificate is opened, go to **Details** tab and click on **Copy to File** button.
- 17) Click **Next** and select **Yes, export the private key option**.



- 18) Click **Next**.

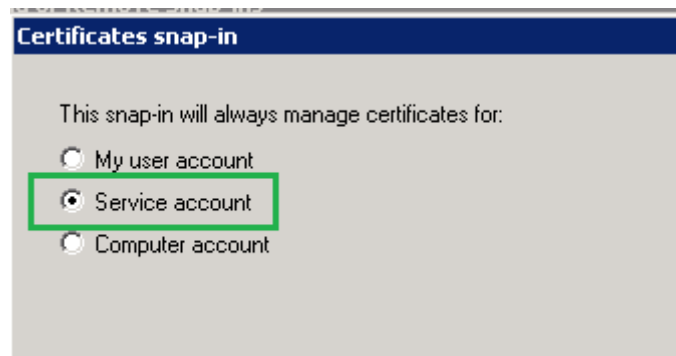


- 19) Enter your password (double time) to assign to the Keystore and click **Next**.
- 20) Save the .pfx file in the system in the same location where certificate request is created for easy identification.
- 21) Click **Next** and click **Finish**.
- 22) In the same *mmc* window, open **File** menu and select **Add/Remove Snap-In** option
- 23) Select **Certificates** and click **Add**.

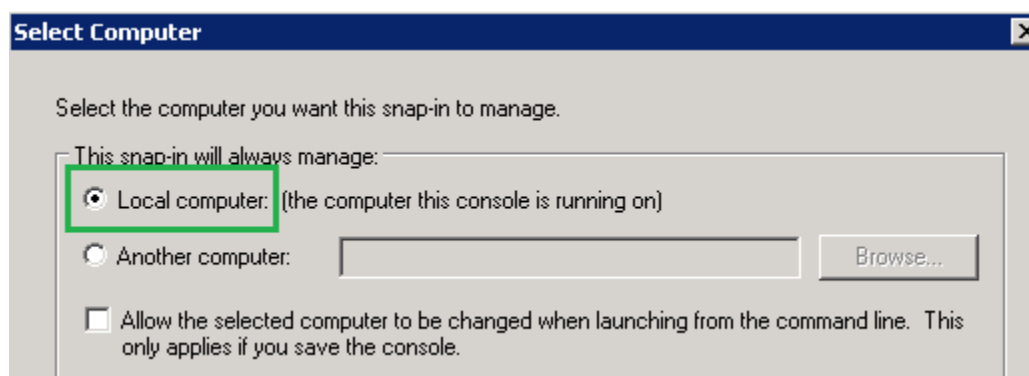


- 24) Select **Service Account**.

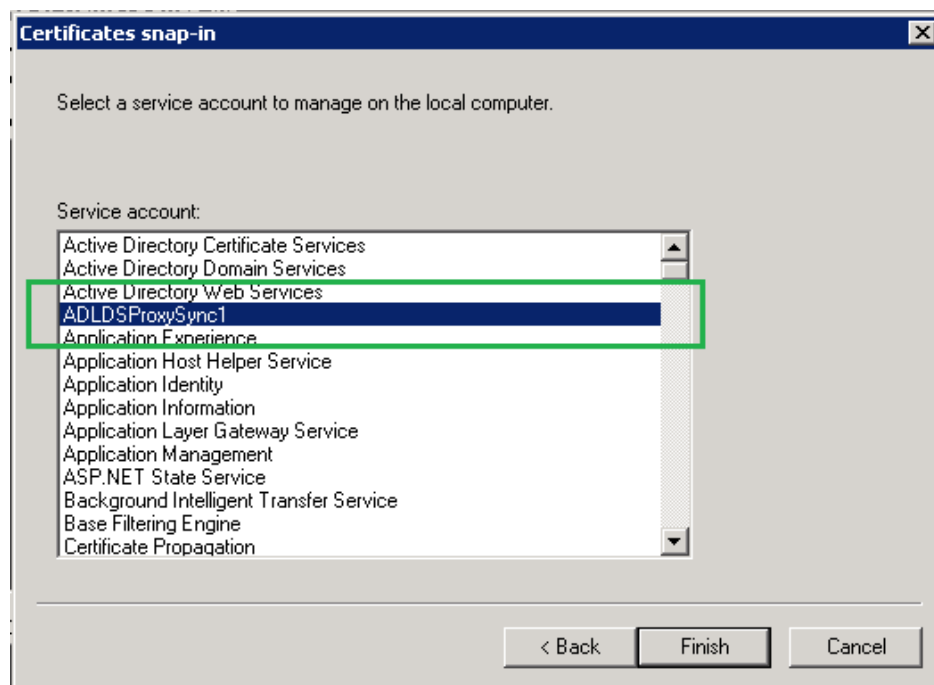




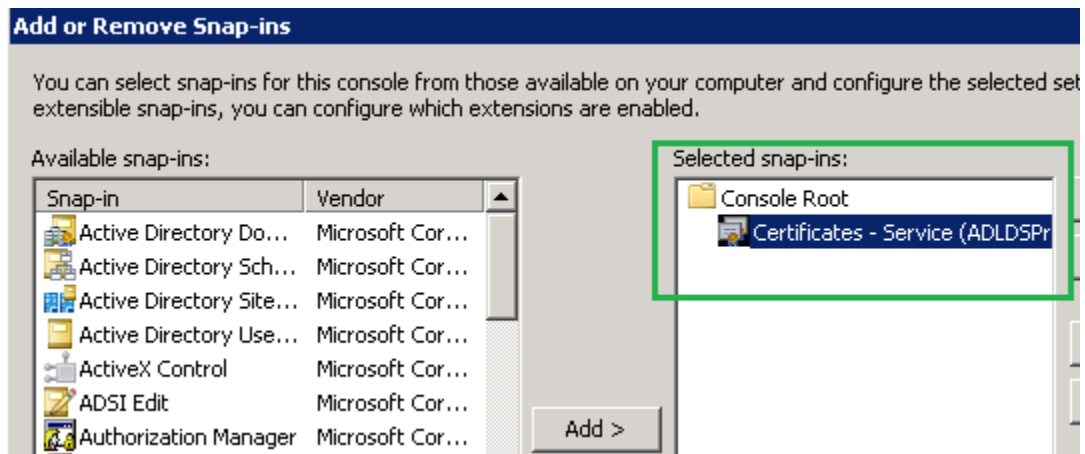
25) Select **Local Computer**, click **Next**.



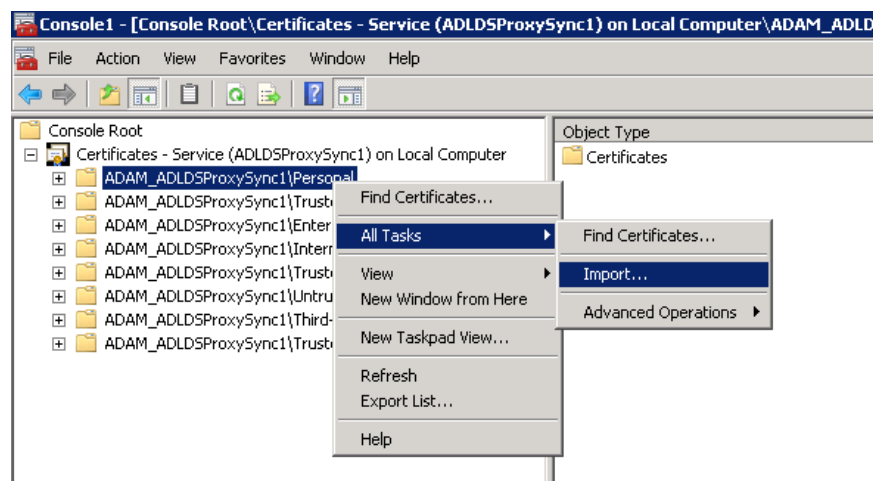
26) Select the Service Name / AD LDS Instance Name.



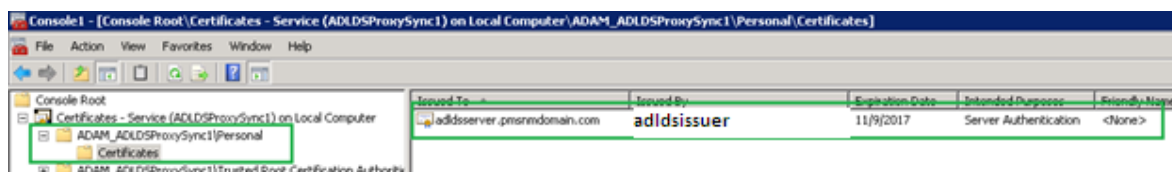
27) Click **Finish** and then click **OK**. The following **Add or Remove Snap-ins** window appears.



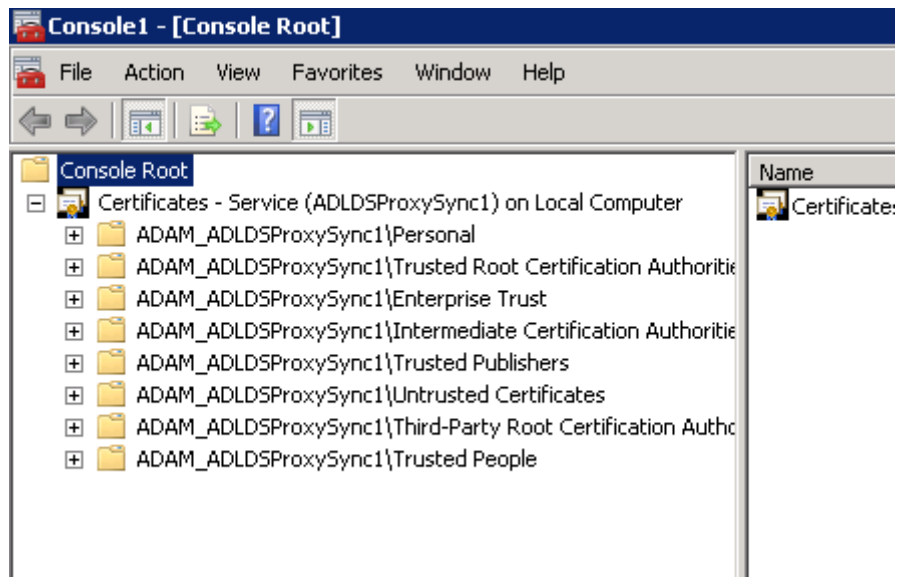
- 28) In mmc **Certificates** window, expand **Certificates – Service (AD LDS Instance Name)** on Local Computer. Add the **AD LDS Signed Certificate** in **AD LDS Instance Name/Personal** section.
- 29) Click **Next > Browse**. Select the key store that you have created in previous step (file extension is .pfx) in File browser.
- 30) Click **Next**. Enter the password of key store (entered while creating .pfx file).
- 31) Click **Next > Next > Finish**.



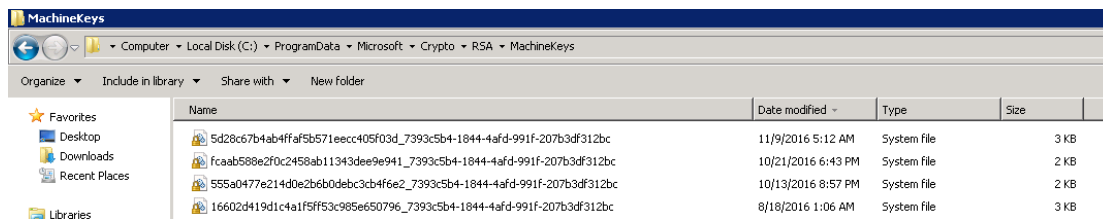
Once it is added, certificate is available as shown below.



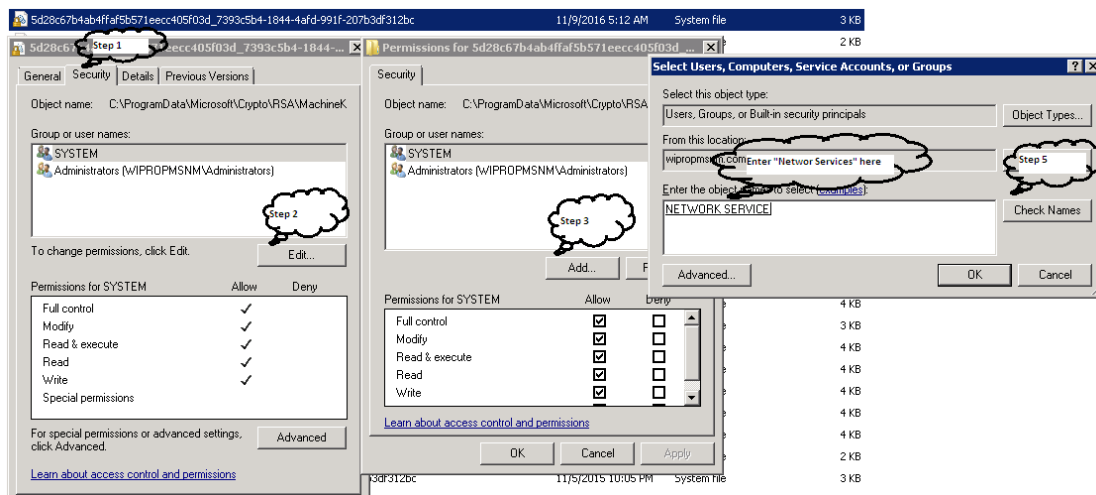
- 32) In the same way, add the **AD LDS certificate's Root certificate** (for example, **pmsnmdomain.com**) in **AD LDS Instance Name/Trusted Root Certificate Authorities**.
- 33) Add the **AD LDS certificate's Root certificate** in **AD LDS Instance Name/Trusted Publishers**.
- 34) Add the other end certificate (for example, Provisioning Manager application certificate) in **AD LDS Instance Name/Trusted People**. An example is shown below.



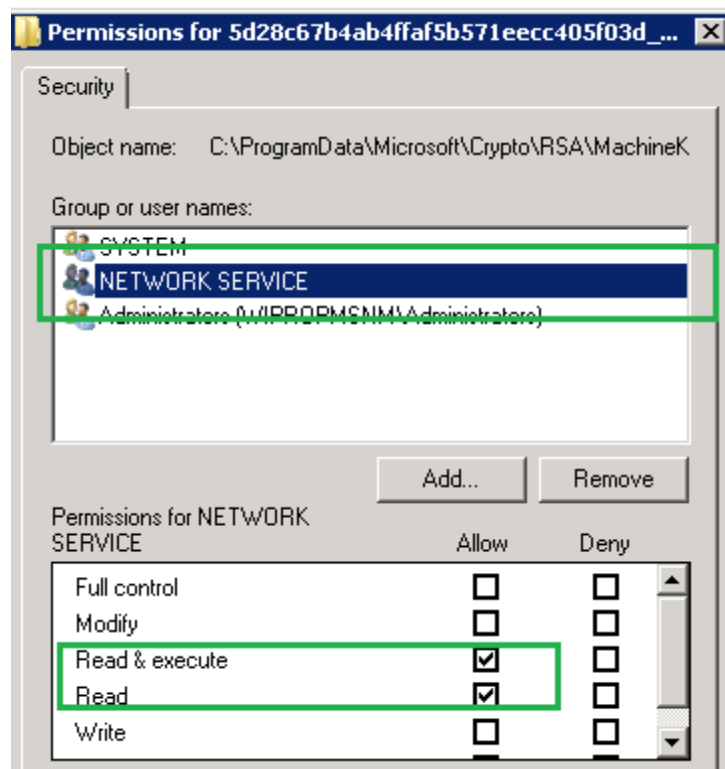
- 35) Add the ownership to the added certificates to **Network Service**.
- 36) Go to C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys.
- 37) Right click on each certificate where **Lock** like icon appears on the files.



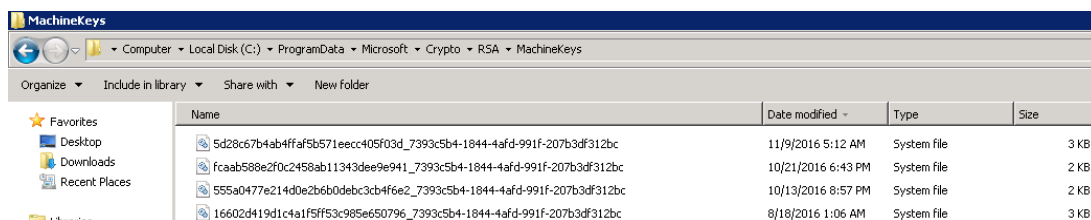
- 38) Open **Properties** and go to **Security** tab. Click **Edit** and then click **Add**. Enter **Network Service**.



- 39) Enter the **Network Service** and select **Users, Computer, and Service Accounts or Groups** window.
- 40) Give **Read, Read & Execute** permission > click **OK** > **OK**.



- 41) In the same way, provide permissions to all certificates for **Network Service** user. When you give the permissions, all the **Lock** icons get disappeared.



- 42) Restart **AD LDS Instance**. Test LDAPS for AD LDS by using the below command from **PM** installed server.

`openssl s_client -connect IPAddress of AD LDS:LDAPS port`

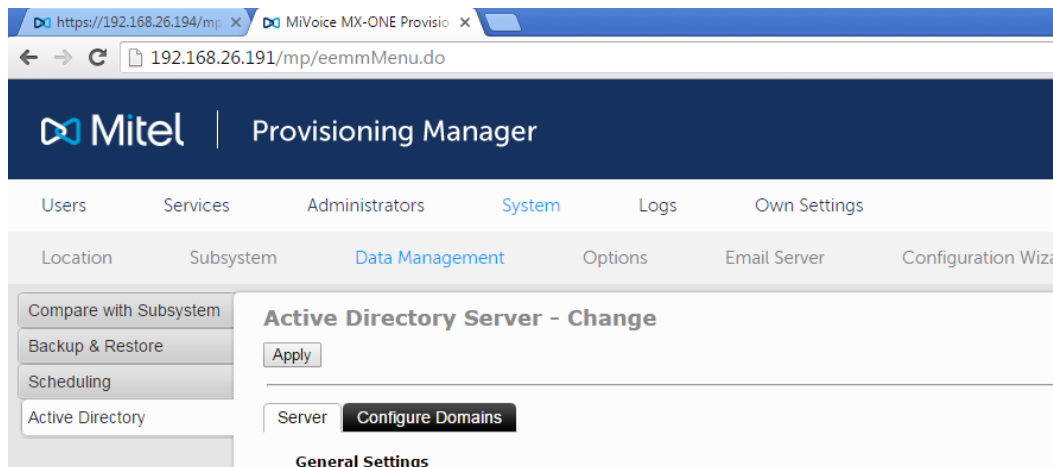
For example:

`openssl s_client -connect 192.168.26.129:53994`

## Using AD LDS as a User Repository in PM Application

To Import Users into PM, do the following:

- 1) Login to **PM** application.
- 2) Select **System** menu > select **Data Management** sub menu > select **Active Directory**.



3) Enter the following fields details.

Server **Configure Domains**

**General Settings**

IP Address: \* 192.168.26.129

Port: 53986

User Name: \* adldsadmin

Password: \*

Confirm Password:

**Notification**

Email Address:

**Rules**

Create Default Password: ☒

Automatically Remove Users: ☒

Scan for Removed Users Interval [m]: 30

**Extension Handling**

Extension/Mailbox Handling: Try assign otherwise create new extension/mailbox

Extension Number Length: 5

**Mailbox Handling**

No OneBox Server subsystem is available. Please initiate through Add Subsystem task.

Add OneBox Server

UDF Mapping: Edit...

**Remove Active Directory Server Configuration**

Remove Configuration

Apply

For example,

- **IP Address:** [IP address of AD LDS Instance located server]
- **Port:** [Normal LDAP port of AD LDS]
- **User Name:** [administrative user created in AD LDS in “Step V”]

- **Password:** [Password of above administrative user]
  - **Confirm Password:** [Type the same password as entered in “Password” field]
- 4) Click on **Apply**. Authentication is Successful is displayed.

**Change operation successful**

Property	Value
<b>General Settings</b>	
IP Address	192.168.26.129
Port	53986
User Name	adldsadmin
<b>Rules</b>	
Create Default Password	Yes
Automatically Remove Users	Yes
Scan for Removed Users Interval [m]	30
<b>Extension Handling</b>	
Extension Number Length	5
<b>Mailbox Handling</b>	
Create Mailbox	Yes

**Configure Domains**  
No property set

Done

- 5) Click **Done**.
- 6) Go to **Configure Domains** tab and click **Add**.

**Domain Configuration - Add**

Apply Cancel

? Search Domains: \*

? Description:

? Select Location : Mitel ▼

? Select parent department for AD deparments : Mitel ▼

**Extension Templates**

Apply Cancel

*Add the following details.*

- Search Domains: [The Domain which is created at AD LDS Side After Step X]

For example, *OU=WBMUSers,DC=wbmusersadldsdomain,DC=com*

- 7) Click **Apply** and then click **Done**.
- 8) Configure the AD LDS Instance details as mentioned below.
- 9) Click **Apply** and then click **Done**.

- 10) Go to **Configure Domains** tab and click on **Synchronization** icon [5th icon from left side].
- 11) Go to **Users** menu and select **User**. Once, the synchronization completed.

- 12) Enter "\*" in **Enter User Name(s), Extension Number, and Department** field.
- 13) Select **Active Directory (AD)** in **Imported from** drop-down list.
- 14) Select **View** to view the list of users who are synchronized from AD LDS.

## Enabling SSL for PM Application

- 1) For the **AD Authentication, Description** refer to the file number *18/1551-ANF 901 15, Section 4 of the CPI Document*.
- 2) Place the certificates of PM at AD LDS side as mentioned in **step XII**.

## Enabling AD Authentication in PM Located Server

For the **AD Authentication, Description** refer to the file number *18/1551-ANF 901 15, Section 4.4* of the CPI Document.

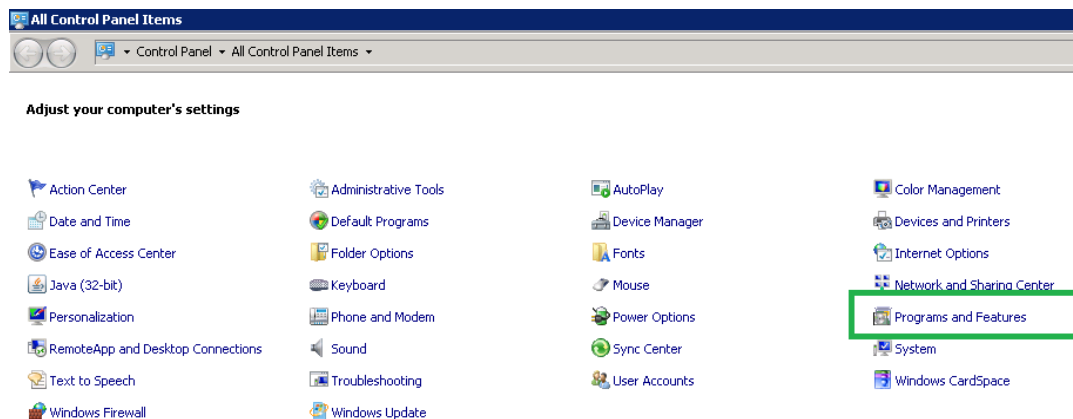
To do this, do as follows:

- 1) Leave the **Principal DN Suffix** field empty.
- 2) Enter LDAPS port of AD LDS in the port field.
- 3) Except this everything is same as we do for Active Directory.
- 4) After this configuration, restart of PM application and try to login with the synchronized users from AD LDS.

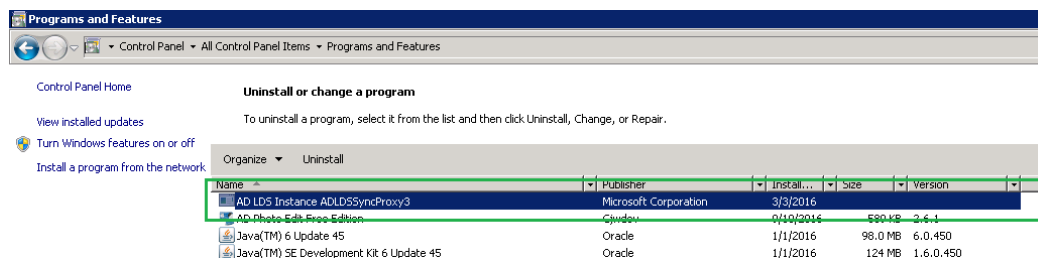
## Uninstalling AD LDS Instance and AD LDS Roles from Server

To uninstall AD LDS Instance from the system, do the following:

- 1) Go to **Control Panel** and select **Programs and Features**.

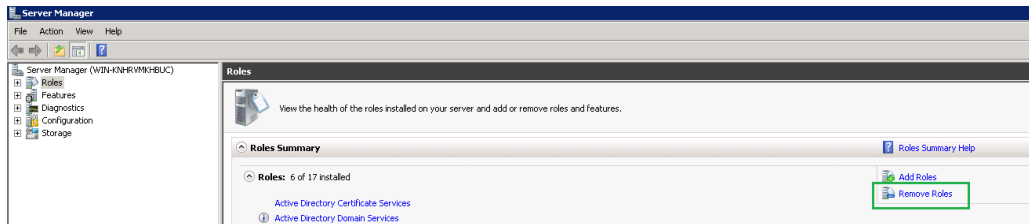


- 2) Select the **AD LDS Instance Name** > select **Uninstall**.

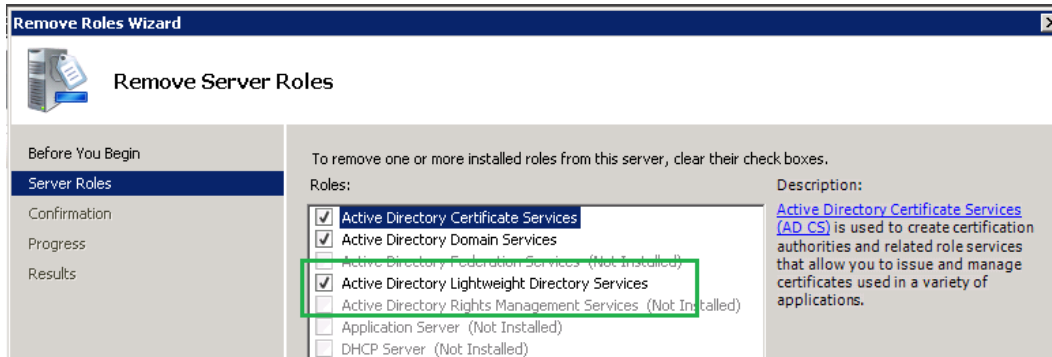


- 3) Remove AD LDS Roles from server.
- 4) Open **Server Manager** and select **Remove Roles**. Click **Next** button in the opened new dialog window.





- 5) Unselect **Active Directory Lightweight Directory Services** check box.



- 6) Click **Next** and then click **Remove** in the next dialog windows.  
7) Click **Close** when it is removed successfully.

