Table of Contents

- Introduction
- Prerequisites
  - Requirements
  - Components Used
- Preface
- Overview
- Active Directory Multiple Forest Support Scenario in CUCM
- Domain Trust Relationship
- Install AD LDS
  - Install AD LDS in 2008
  - Install AD LDS in 2012
- Install the Instance for Multiple Forest Support
  - Multiple Forest Support in 2008
  - Multiple Forest Support in 2012
- Configure ADAM Schema Analyzer
- Extend the AD LDS Schema with the User-Proxy Objects
- Import the Users From AD DC to AD LDS
- Create the User in AD LDS for CUCM Synchronization and Authentication
- Configure Bind Redirection
- Configure CUCM
- LDAP Filters in CUCM

Introduction

This document discusses how to configure Cisco Unified Communication Manager (CUCM) Directory Integration in a Multi-Forest Environment.

Prerequisites

Requirements

Cisco recommends that you have:

1. Knowledge of deployment and configuration of CUCM directory integration.
2. Knowledge of deployment and configuration of Microsoft Active Directory Application Manager (ADAM) 2003 or Microsoft Lightweight Directory Services (AD LDS) 2008 or 2012.

3. CUCM Release 9.1(2) or later.
4. When you use CUCM Release 9.1(2) or later, the LDAP filter can be changed with the Administrative web interface.
5. The number of user accounts to be synchronized must not exceed 60,000 accounts per CUCM Publisher. When more than 60,000 accounts need to be synchronized, the IP Phone Services Software Development Kit (SDK) must be used in order to provide a custom directory. See the Cisco Developer Network for additional details. When you use Unified CM Release 10.0(1) or later, the maximum number of user accounts supported is 160,000.
6. Microsoft ADAM 2003 or Lightweight Directory Services (LDS) 2008 or 2012.
7. The requirement for SSL when you use bind redirection should not be disabled. If it is disabled, it causes the password of a Windows security principal to pass to the computer that runs ADAM without encryption. Thus, it should be disabled only in a test environment.
8. User ID (sAMAccountName) needs to be unique across all the forests as multiple directory partition is not supported.
9. If there is an AD LDS setup and if the CUCM UserID mapped to sAMAccountName needs to be used, then that agreement should be configured as the AD.
10. When you configure the domain trust relationship between ADAM instance host domain and user accounts host domain, the domain functional level and the forest functional level should be 2003 or later.
11. CUCM supports only a single application directory partition in AD LDS, multi partition is not supported currently.

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

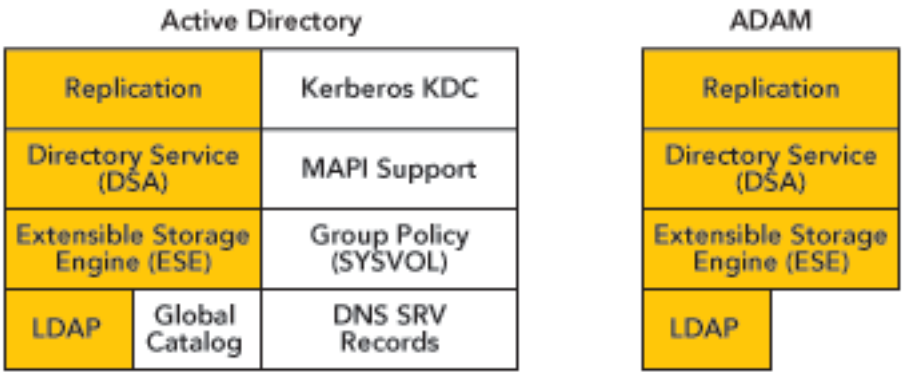
Preface

Microsoft AD LDS, formerly known as ADAM, can be used to provide directory services for directory-enabled applications. Instead of using your organization's Active Directory Domain Service (AD DS) database in order to store the directory-enabled application data, AD LDS can be used to store the data. AD LDS can be used in conjunction with AD DS so that you can have a central location for security accounts (AD DS) and another location in order to support the application configuration and directory data (AD LDS). With AD LDS, you can reduce the overhead

associated with AD replication, you do not have to extend the AD schema in order to support the application, and you can partition the directory structure so that the AD LDS service is only deployed to the servers that need to support the directory-enabled application.

- Install from Media Generation - The ability to create installation media for AD LDS with Ntdsutil.exe or Dsdbutil.exe.
- Audit - Audit changed values within the directory service.
- Database Mounting Tool - Gives you the ability to view data within snapshots of the database files.
- AD Sites and Services Support - Gives you the ability to use AD Sites and Services in order to manage the replication of the AD LDS data changes.
- Dynamic List of LDIF files - With this feature, you can associate custom LDIF files with the current default LDIF files used for setup of AD LDS on a server.
- Recursive Linked-Attribute Queries - LDAP queries can follow nested attribute links in order to determine additional attribute properties, such as group memberships.

There are a lot of differences between ADAM and AD, ADAM can only deliver part of the functions delivered by AD.



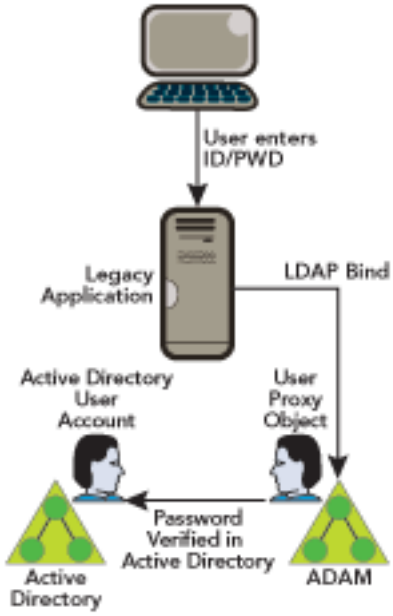
Overview

The objective of this document is to explain the mechanisms that allow CUCM, or any other Cisco products that use Directory Integration Service (DirSync), to get user information and perform authentication from different AD domains that can exist in different forests. In order to achieve this objective, ADAM is used in order to synchronize its user database with different AD Domain Controllers or other LDAP sources.

ADAM can create a database of users and store their details. Single Sign On (SSO)

functionality is desired in order to avoid end users having to maintain different sets of credentials in different systems; therefore, ADAM bind redirection is used. ADAM bind redirection is a special function for applications that support LDAP bind as an authentication mechanism. In some cases, the special schema, or naming context, might force you to avoid AD, which makes ADAM a necessary choice. This avoids users having to remember multiple passwords due to the employment of an additional directory with its own user ID and password.

A special user proxy object in ADAM maps to a regular AD user account. The user proxy does not have an actual password stored in the ADAM object itself. When the application performs its normal bind operation, it checks the ID locally, but checks the password against AD under the covers as shown in this figure. The application does not need to be aware of this AD interaction.



ADAM bind redirection should be used only in special cases where an application can perform a simple LDAP bind to ADAM. However, the application still needs to associate the user with a security principal in AD.

ADAM bind redirection occurs when a bind to ADAM is attempted with use of a special object called a proxy object. A proxy object is an object in ADAM that represents a security principal in AD. Each proxy object in ADAM contains the SID of a user in AD. When a user attempts to bind to a proxy object, ADAM takes the SID that is stored in the proxy object, together with the password that is supplied at bind time, and presents the SID and the password to AD for authentication. A proxy object in ADAM does not store a password, and users cannot change their AD passwords through ADAM proxy objects.

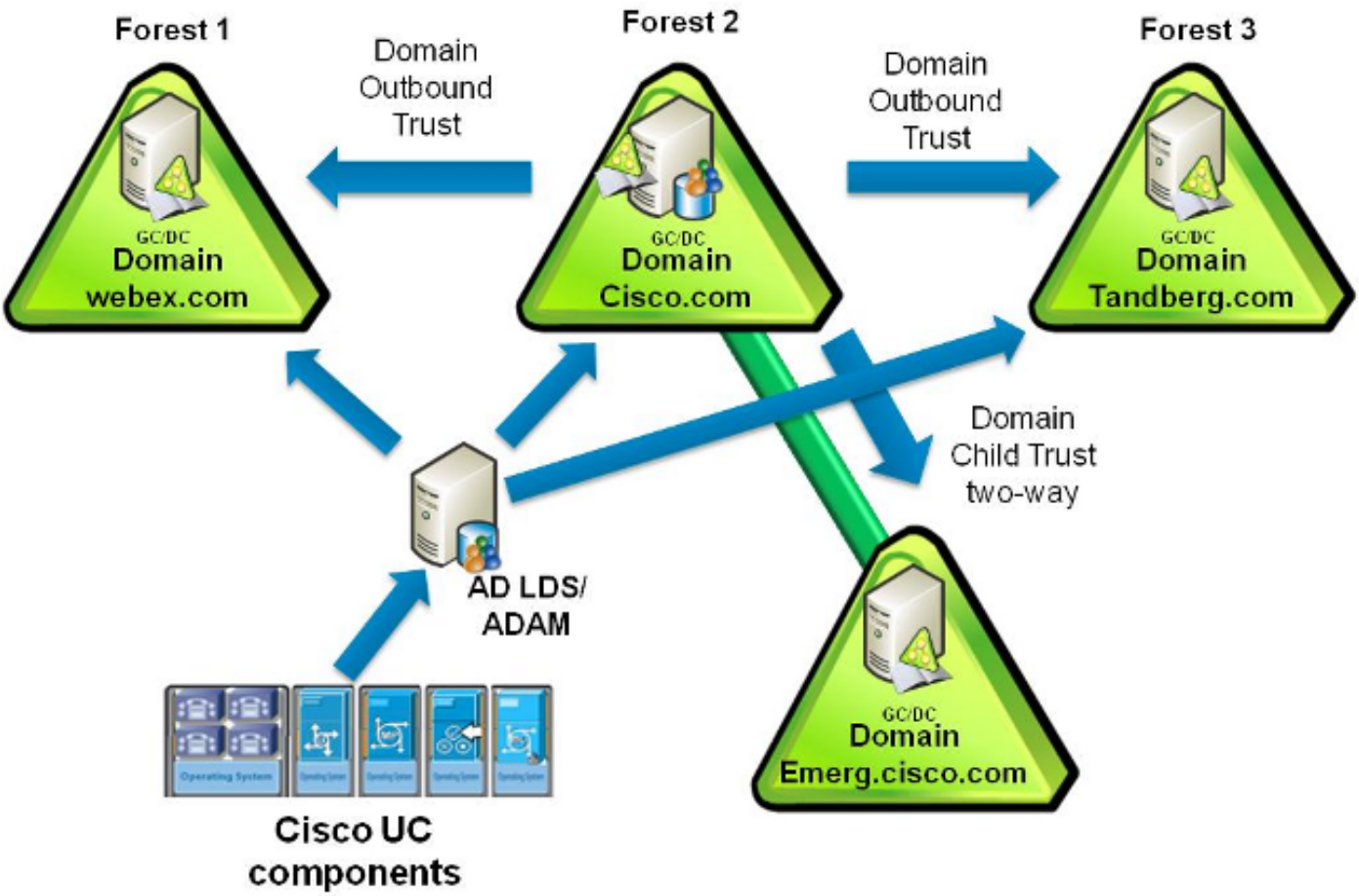
The password is presented in plain text to ADAM because the initial bind request is a simple LDAP

bind request. For this reason, an SSL connection is required by default between the directory client and ADAM. ADAM uses Windows Security APIs in order to present the password to AD.

You can get more information on bind redirection in Understanding ADAM bind redirection .

Active Directory Multiple Forest Support Scenario in CUCM

In order to explain the method, imagine a scenario where Cisco Systems (Forest 2) has acquired two other companies: Tandberg (Forest 3) and Webex (Forest 1). In the migration phase, integrate the AD structure of each company in order to allow the deployment of a single Cisco Unified Communications cluster.



In the example, company Cisco (Forest 2) has two domains, Forest root domain called CISCO (dns cisco.com) and a subdomain called EMERG (dns emerg.cisco.com). Both of these domains have a Domain Controller that is also a Global Catalog, and each one is hosted in Windows 2008 Server SP2.

Company Tandberg (Forest 3) has a single domain with a Domain Controller that is also a Global Catalog, and it is hosted in Windows 2008 Server SP2.

Company Webex (Forest 1) has a single domain with a Domain Controller that is also a Global Catalog, and it is hosted in Windows 2003 R2 Server SP2.

AD LDS is installed in the Domain Controller for domain CISCO, or can be a separate machine; in fact it could be anywhere in one of the three forests. The DNS infrastructure must be in place such that domains in one forest can communicate with domains in other forests and to establish the appropriate trust relationships and validations between the forests.

Domain Trust Relationship

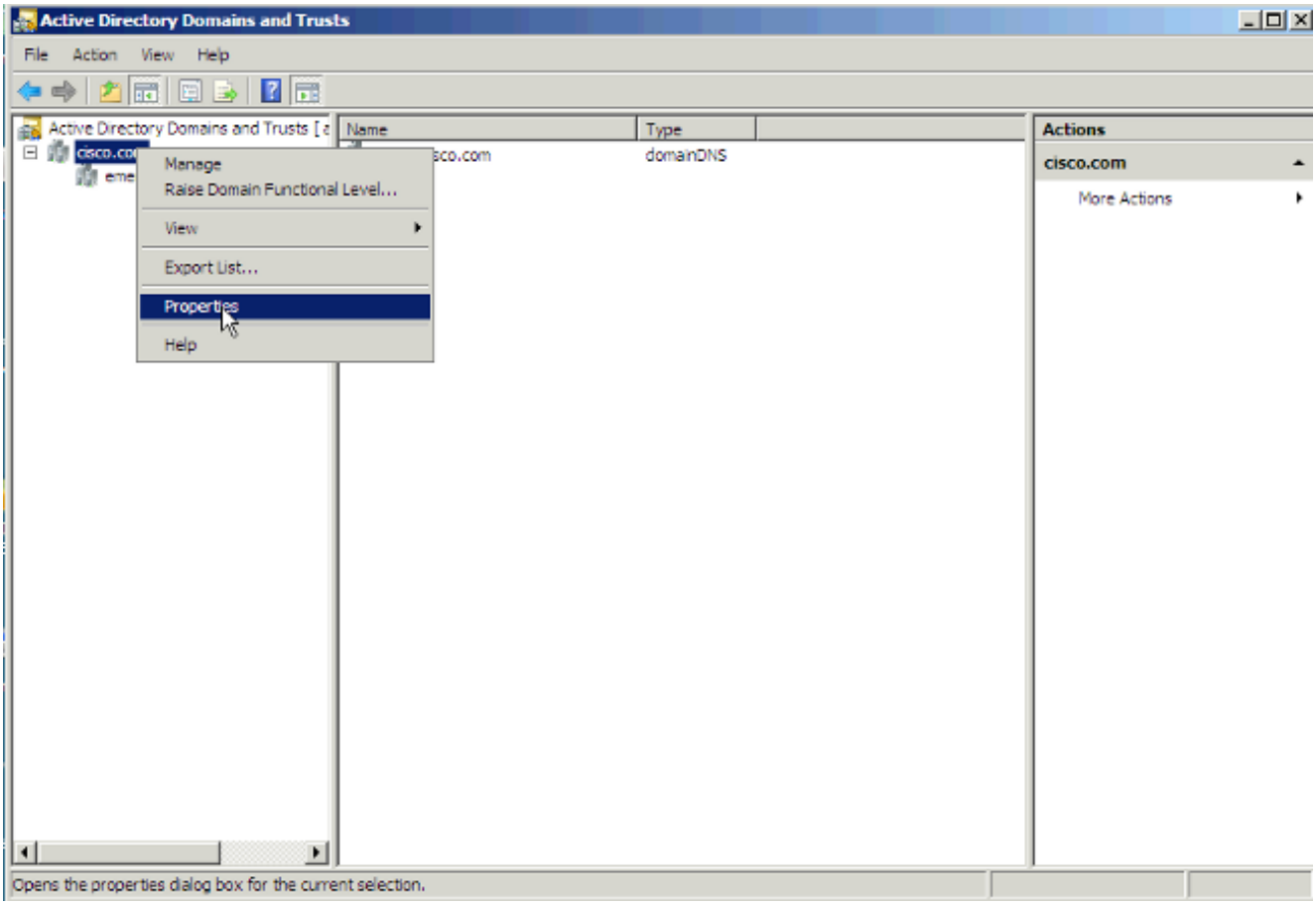
For the authentication of the users to work, you need to have a trust between the domain where the ADAM instance is hosted, and the other domain(s) that hosts the user accounts. This trust can be a one-way trust if required (outgoing trust from the domain that hosts the ADAM instance to the domain(s) that hosts the user accounts). This way, the ADAM instance will be able to forward the authentication requests to DCs in those account domains.

Furthermore, you will need to have a user account from both account domains that has access to all attributes of all user accounts in the domain. This account is used by ADAMSync in order to synchronize the Account Domain users to ADAM.

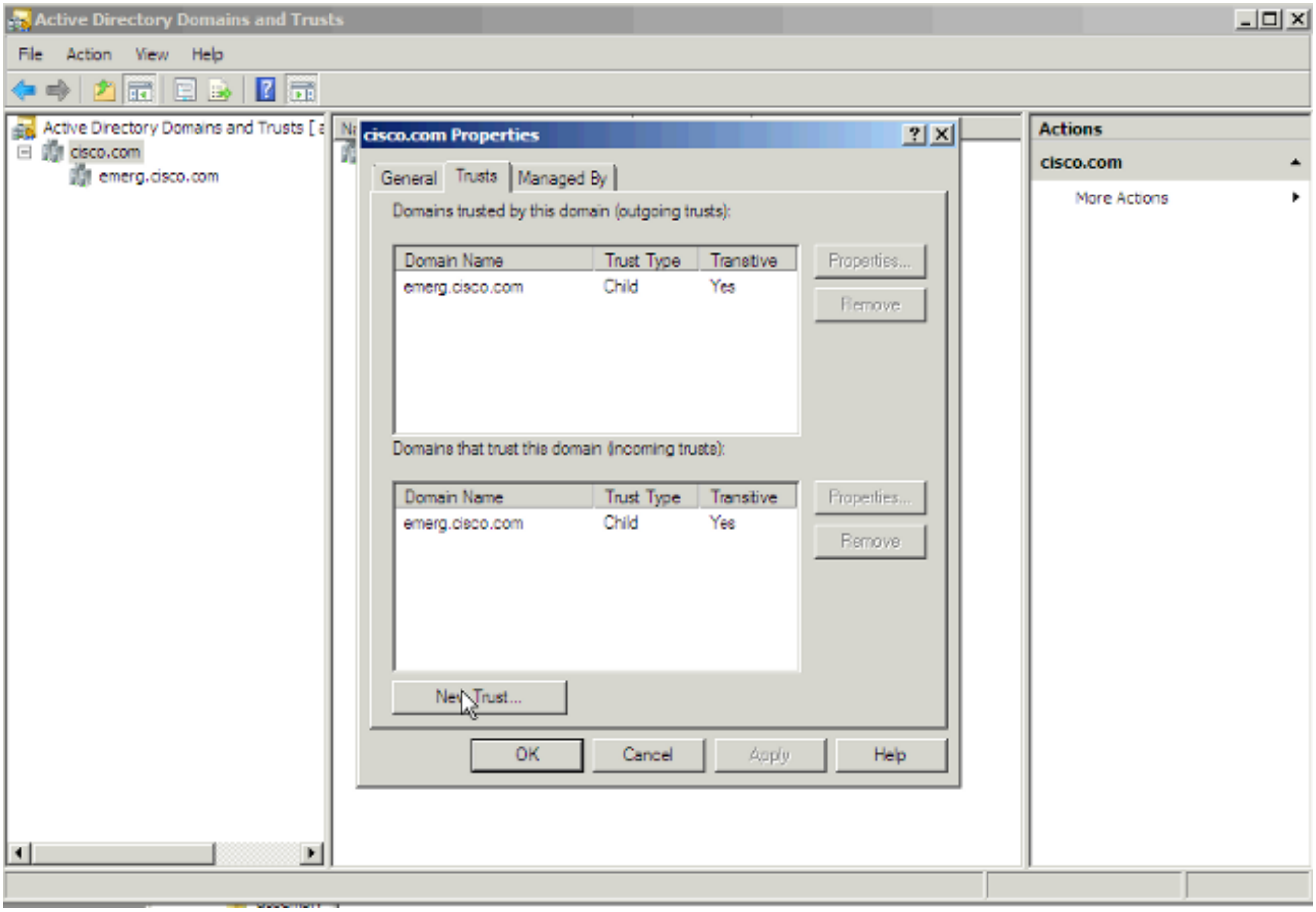
Last but not least, the machine that runs ADAM must be able to find all domains (DNS), find domain controllers in both domains (with DNS), and connect to these Domain Controllers.

Complete these steps in order to set up the intertrust relationships:

1. Open Active Directory Domains and Trusts, right-click the domain that hosts AD LDS, and choose **Properties**.

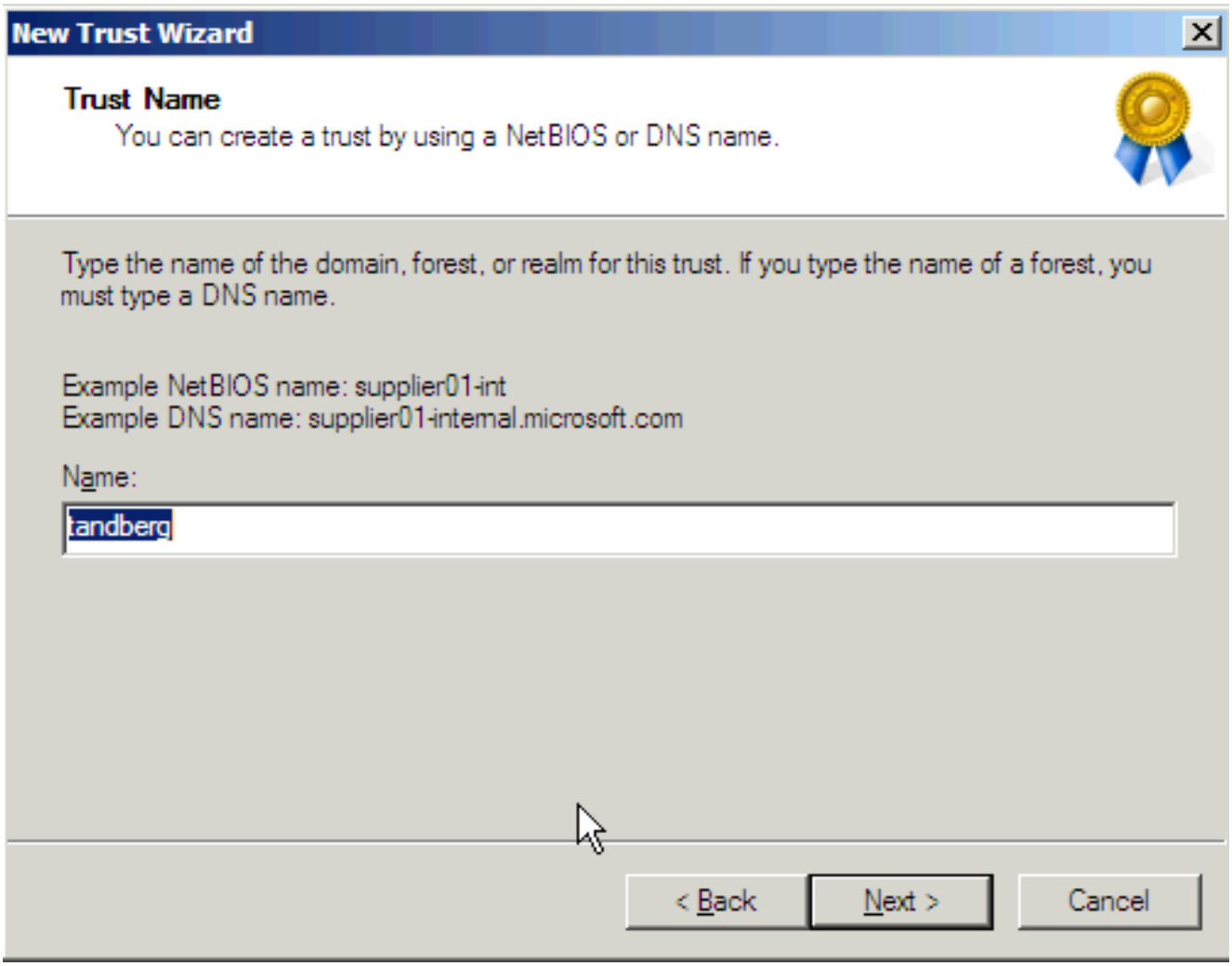


2. Click the **Trusts** tab, and click **New Trust**.

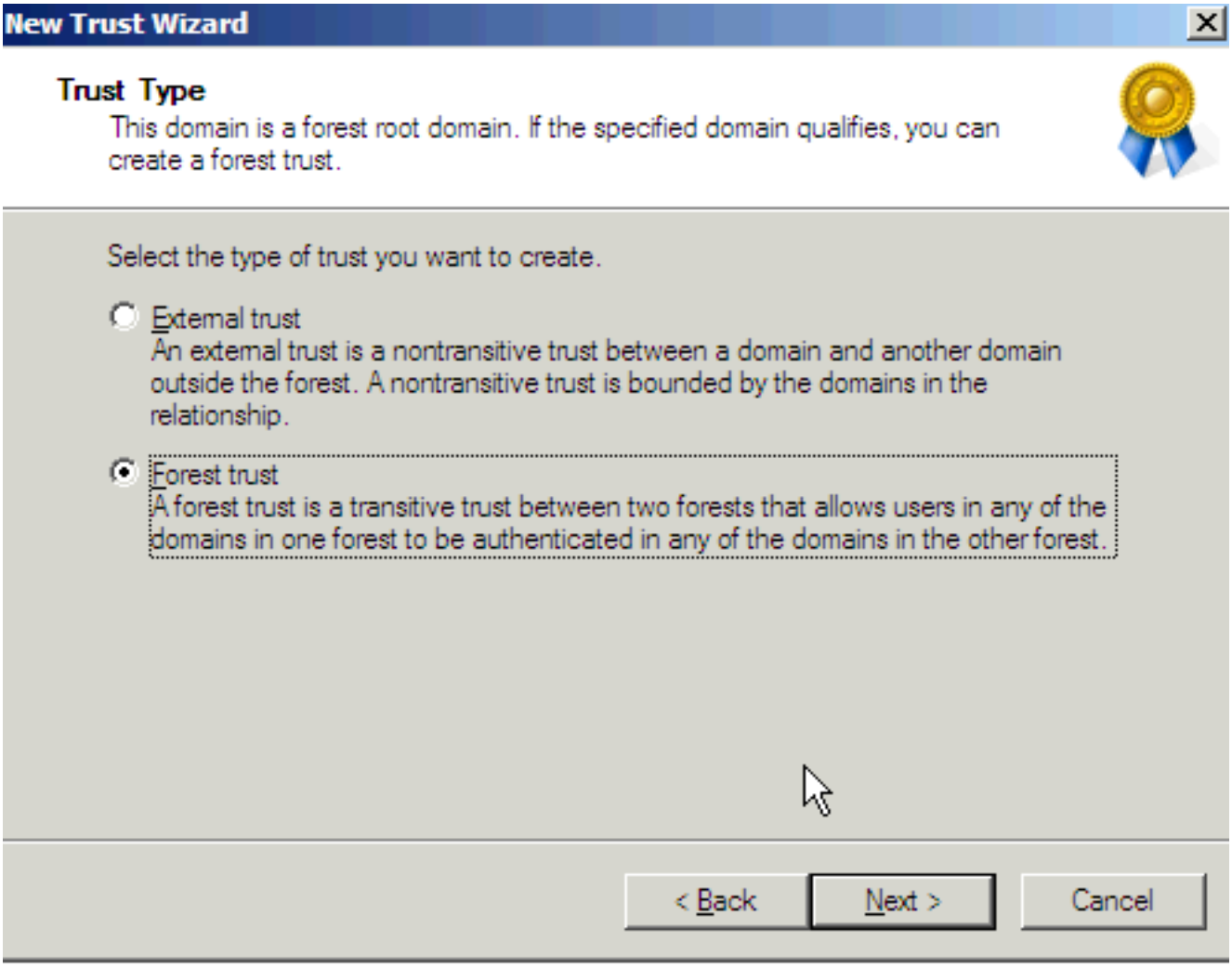


3. Follow the wizard and enter the name of the domain that you want to establish the trust with.

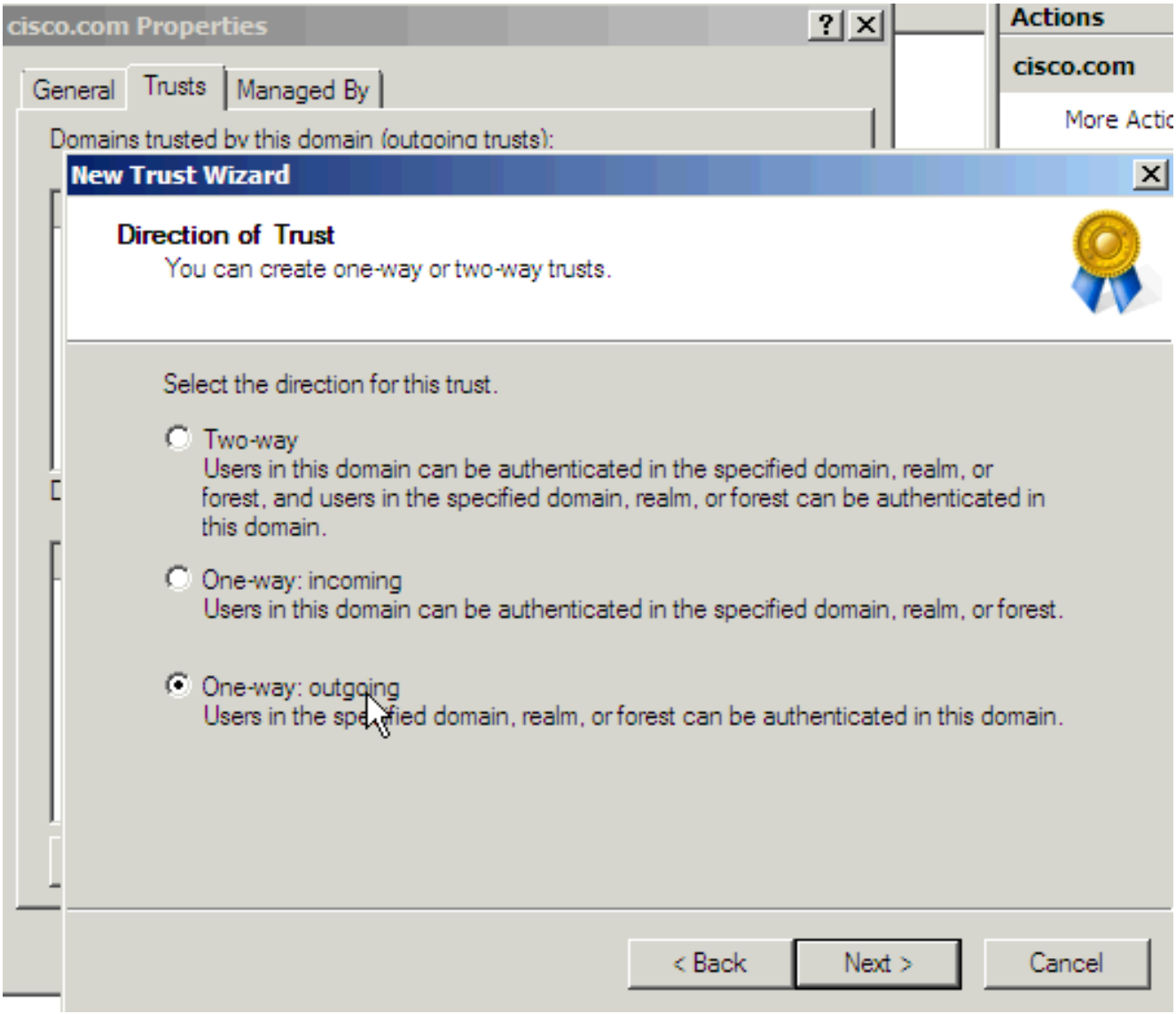
Click **Next**.



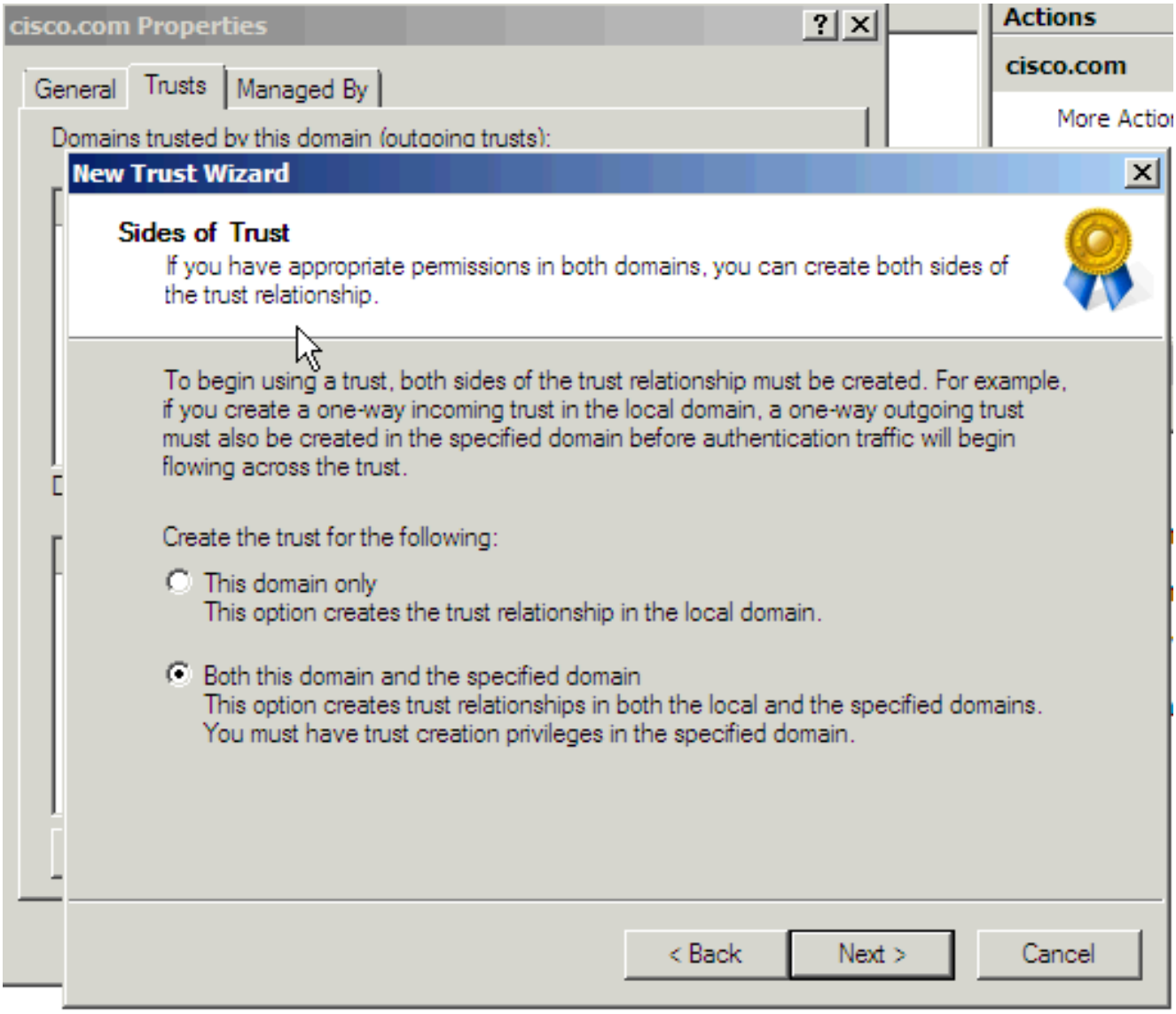
4. Click the **Forest trust** radio button. Click **Next**.



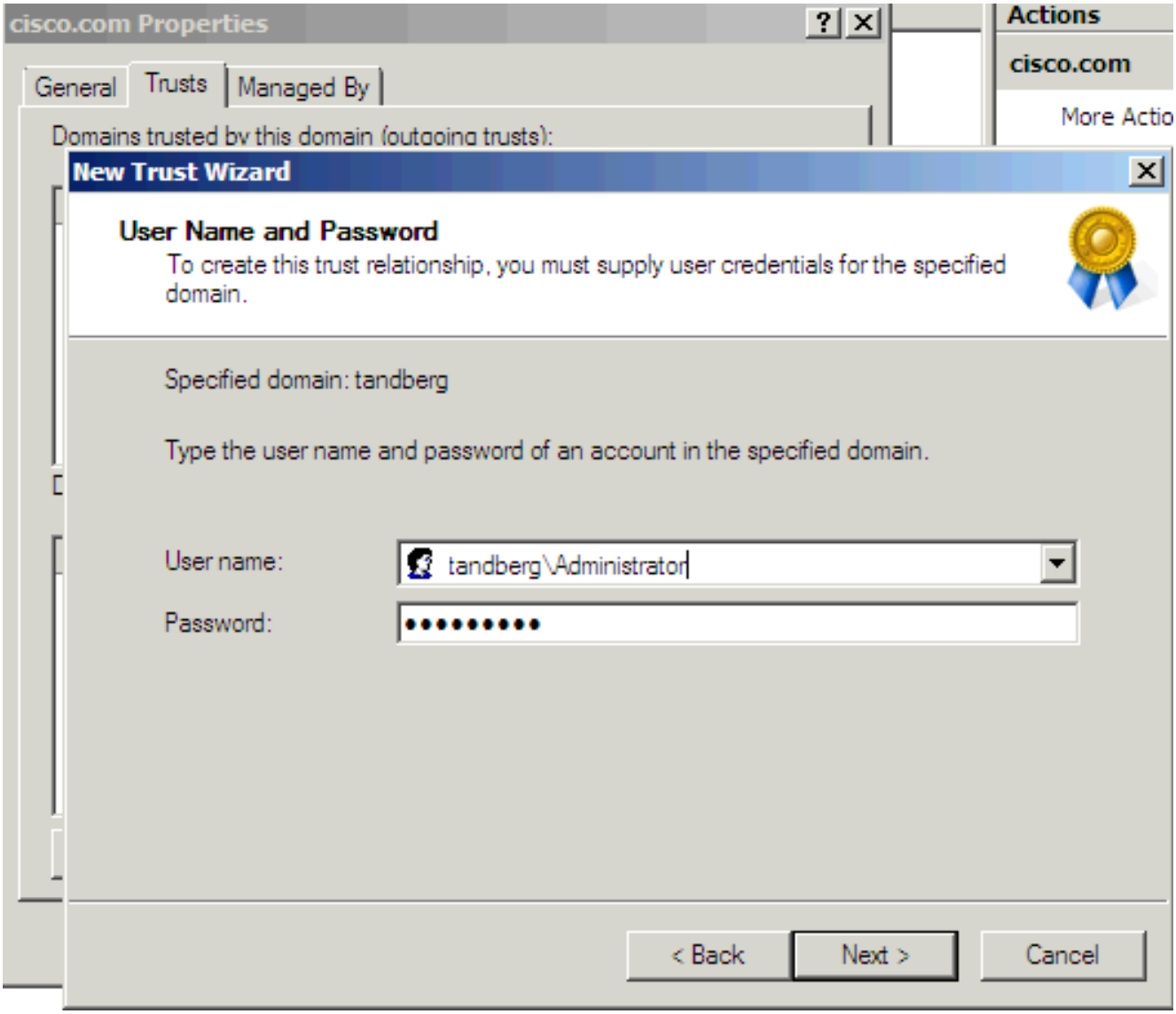
5. On the direction of the trust only 'one-way: outgoing' is required. Click the **One-way: outgoing** radio button. Click **Next**.



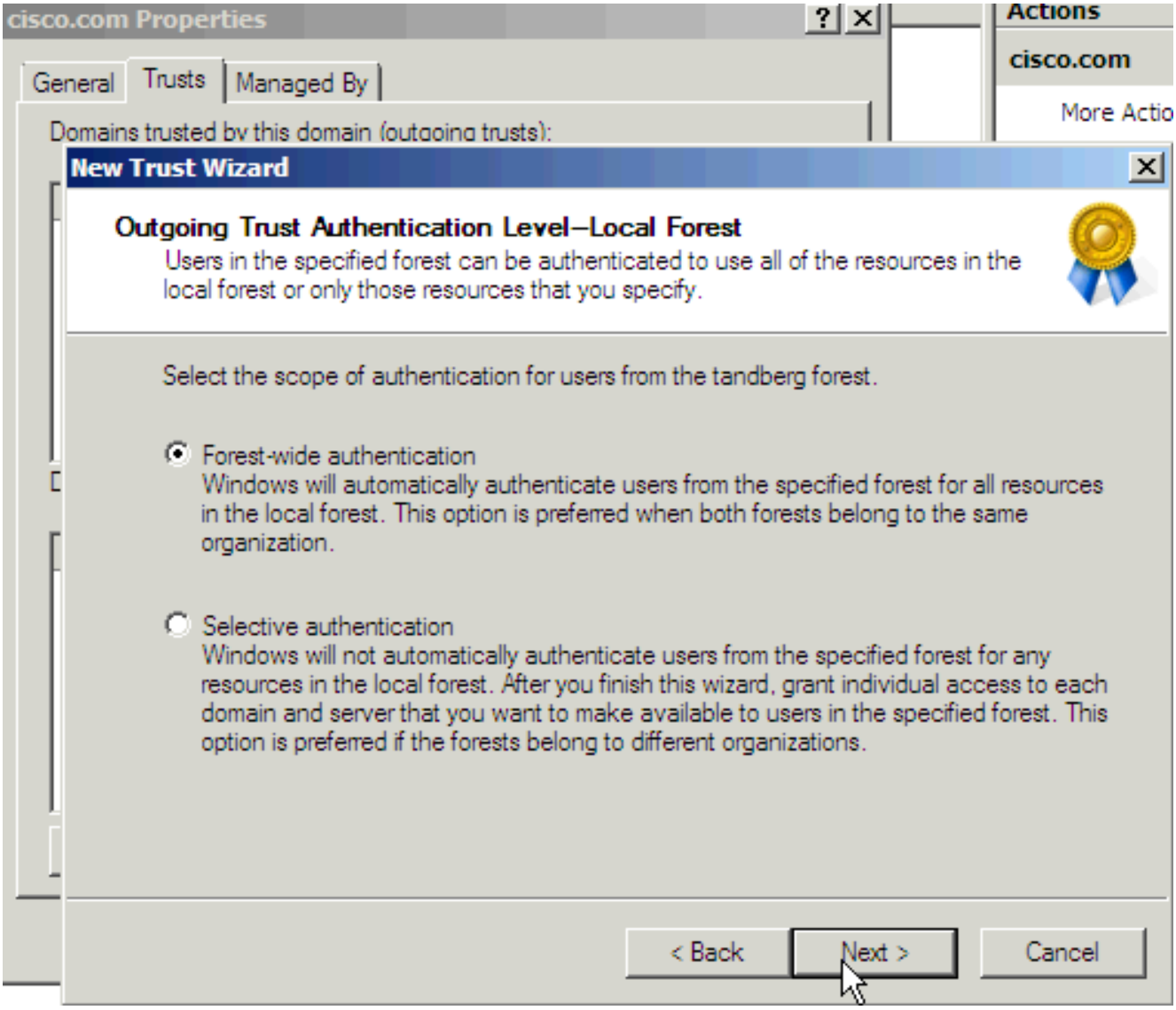
6. Allow the wizard to configure both domains. Click the **Both this domain and the specified domain** radio button. Click **Next**.



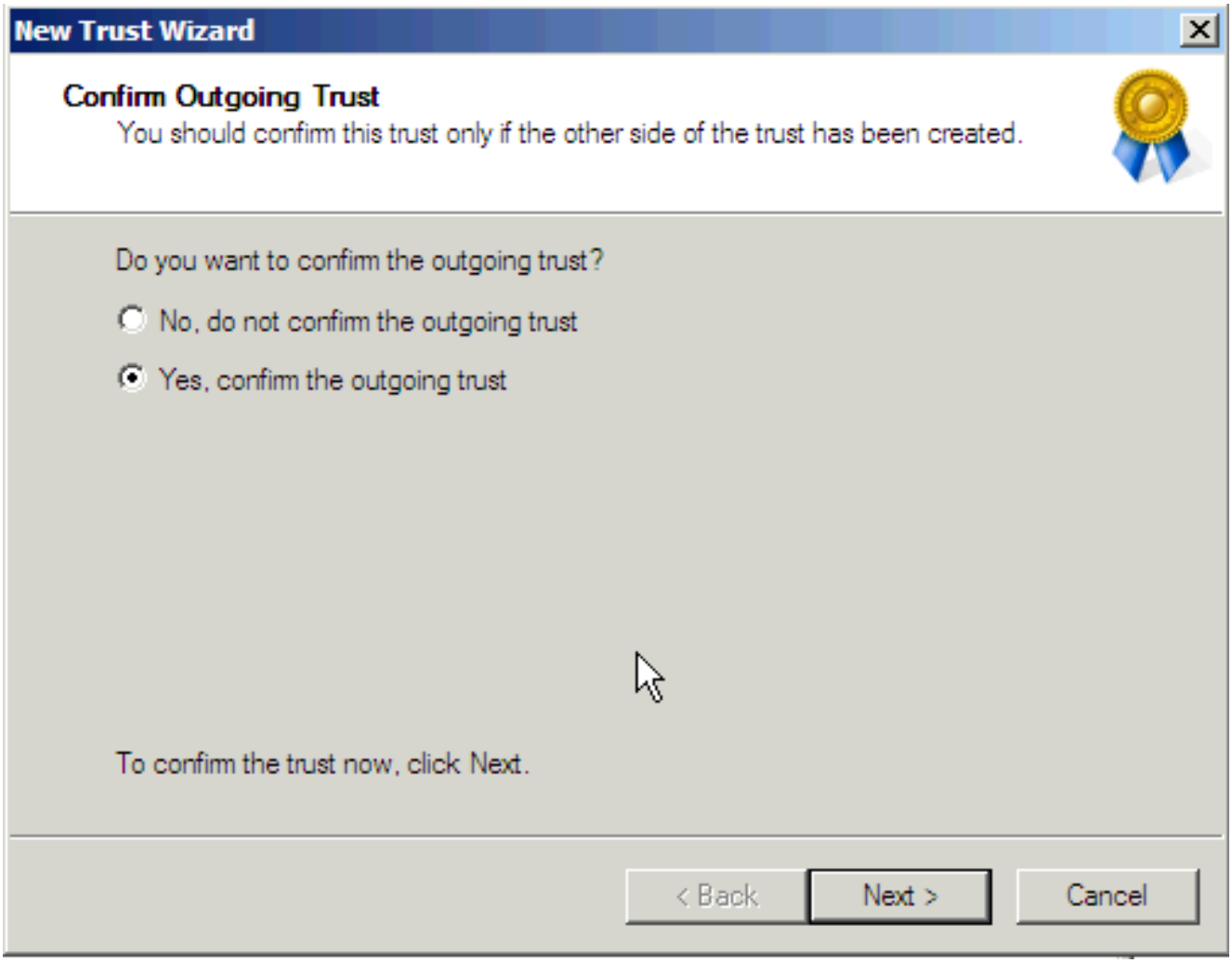
7. Enter the credentials for the other domain. Click **Next**.



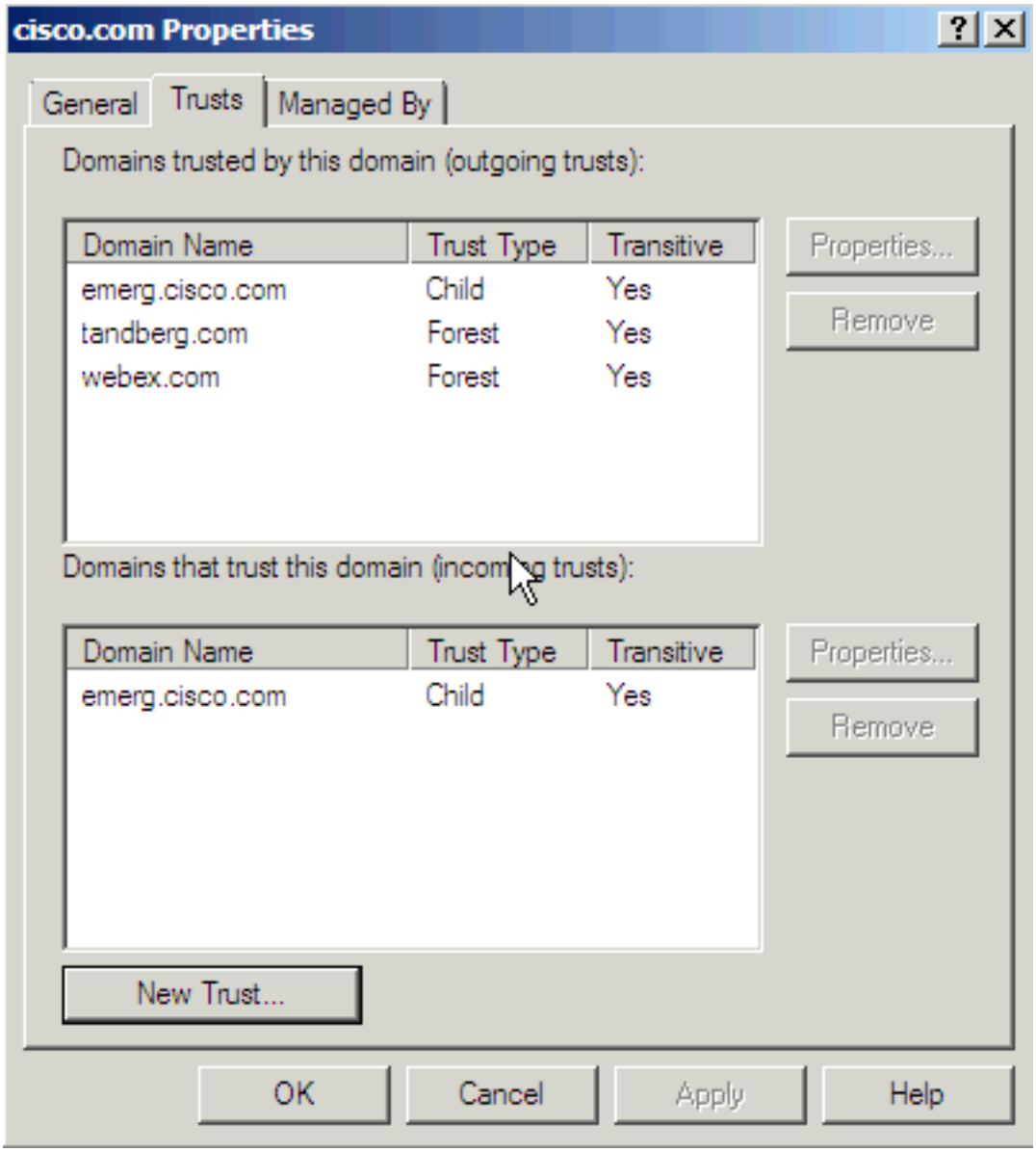
8. Click the **Forest-wide authentication** radio button. Click **Next**.



9. Click the **Yes, confirm the outgoing trust** radio button. Click **Next**.



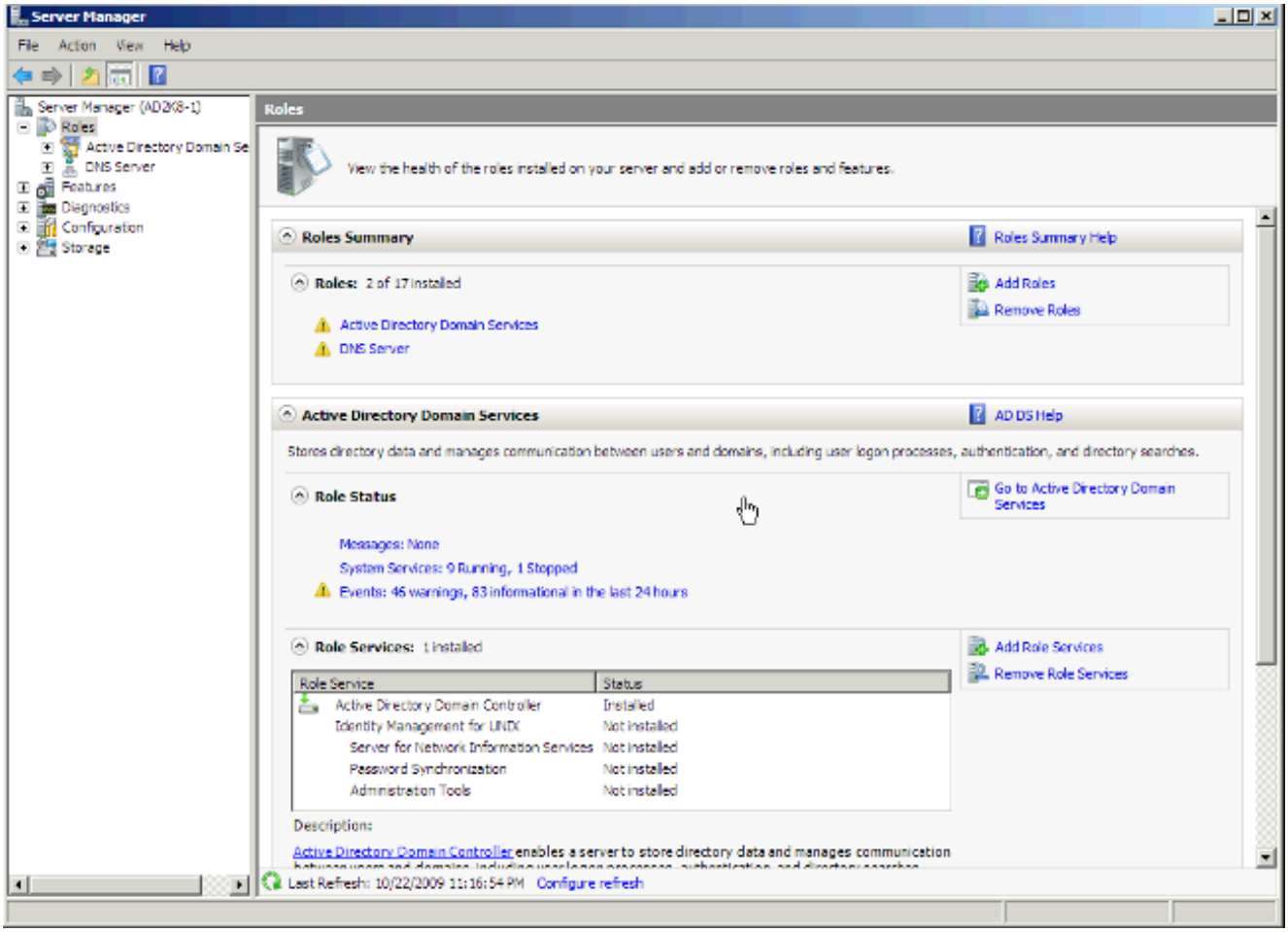
This is the result that you receive after you run this process for both the Tandberg and Webex domains. The domain emerg is there by default since it is a child domain. Click **OK**.



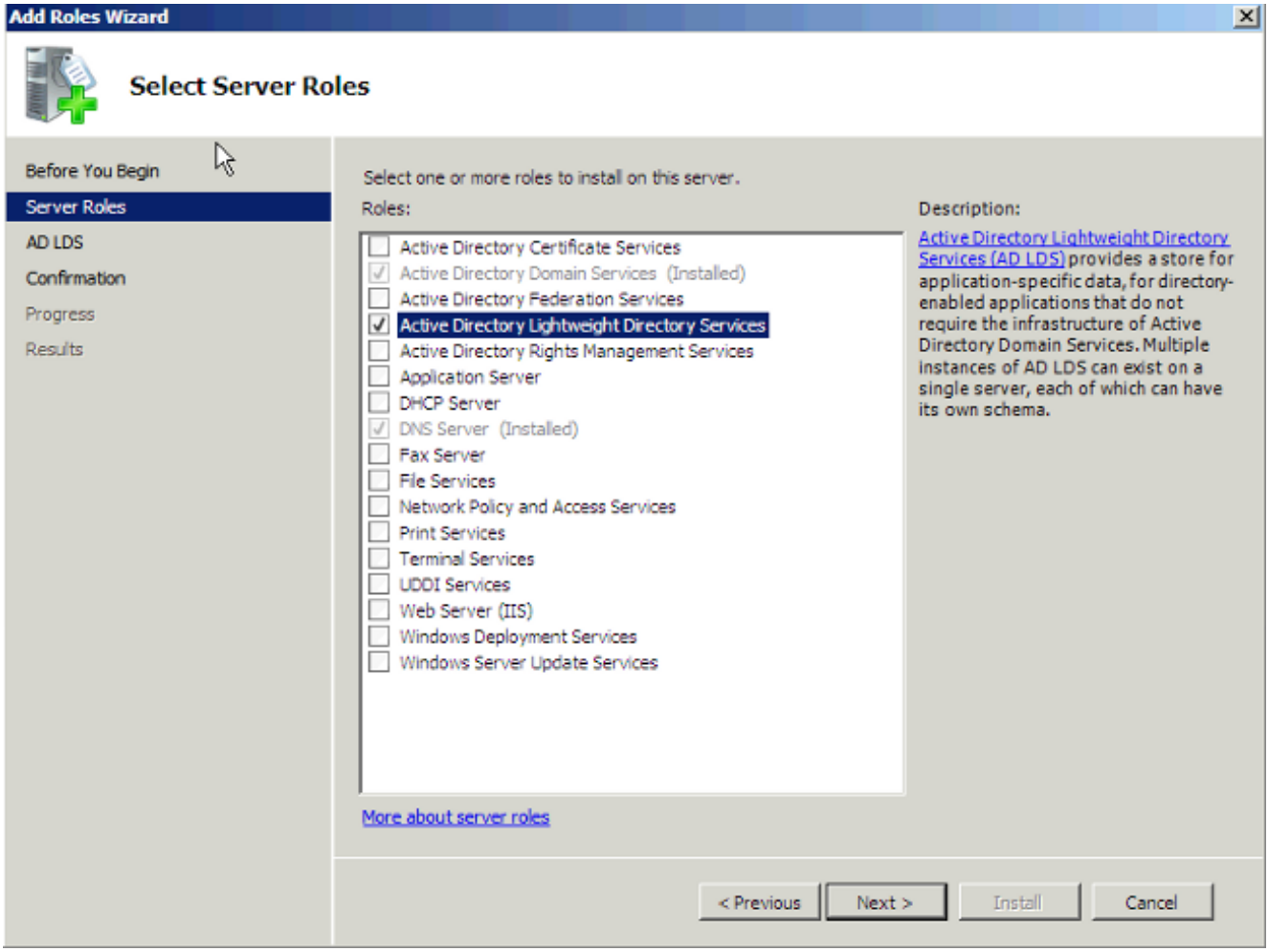
Install AD LDS

Install AD LDS in 2008

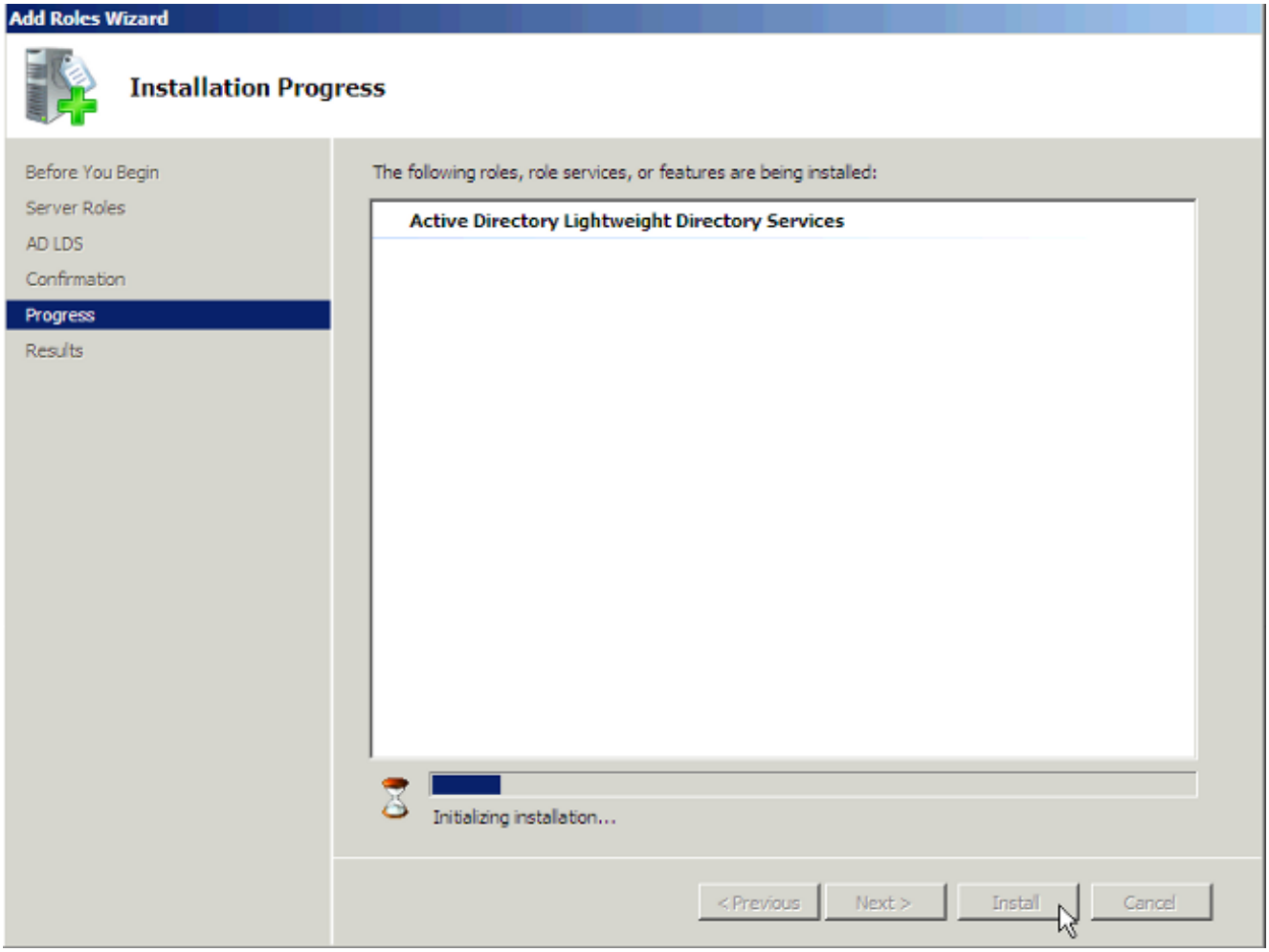
1. Open Server Manager, click **Roles**, and click **Add Roles**.



2. Check the **Active Directory Lightweight Directory Services** check box. Click **Next**.



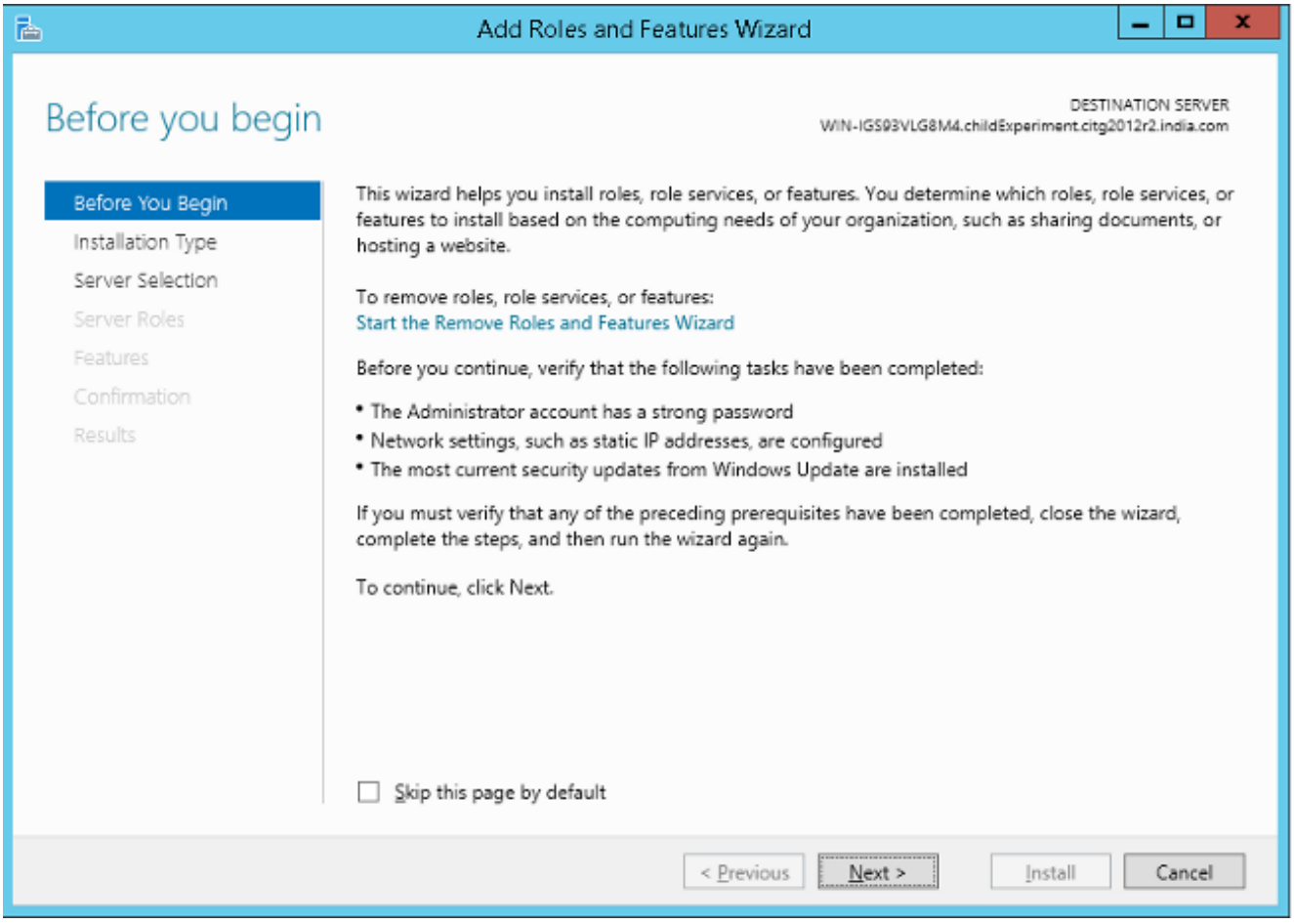
3. The AD LDS Services Installation Progress window appears.



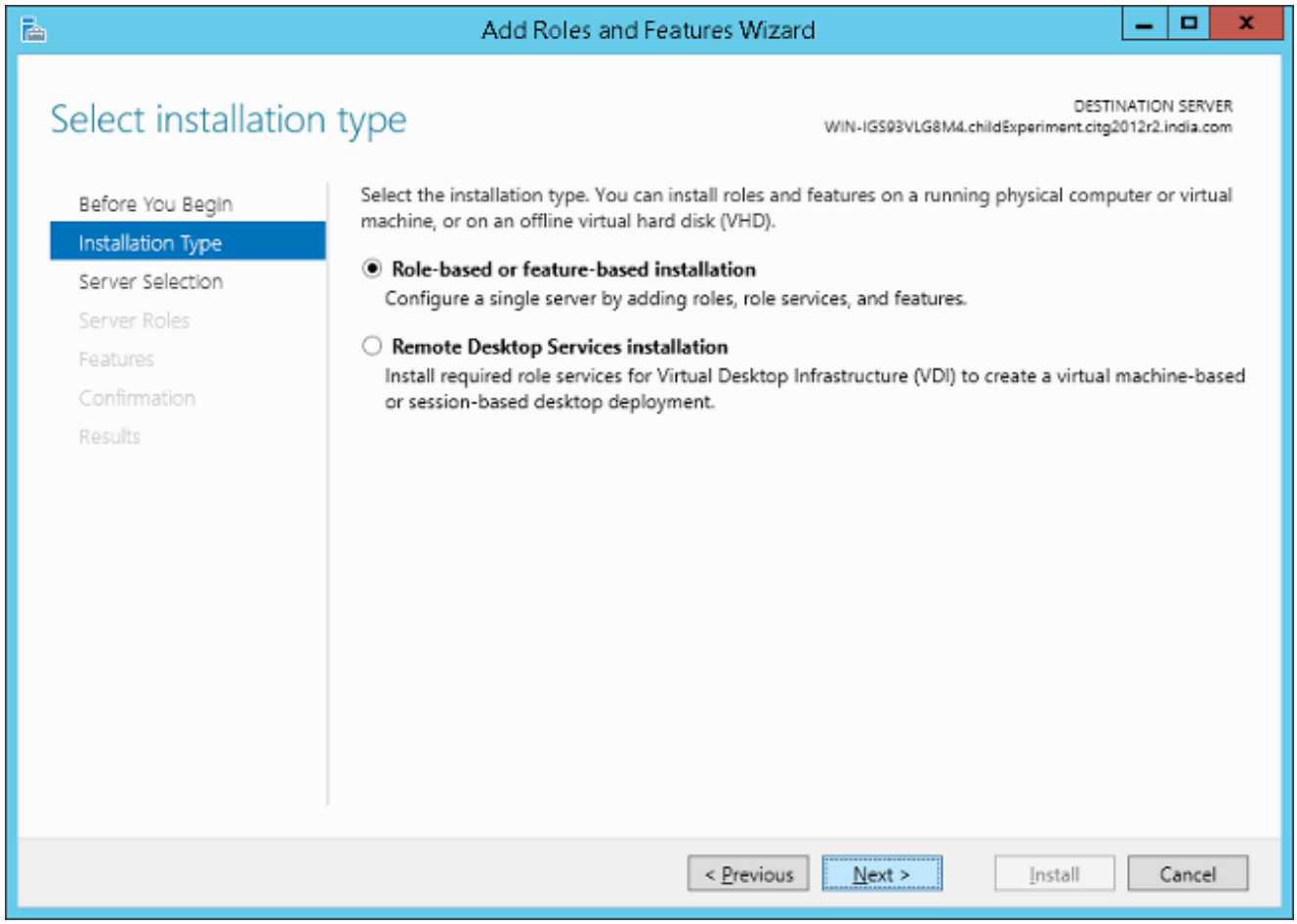
Install AD LDS in 2012

Complete these steps in order to set up AD LDS in 2012:

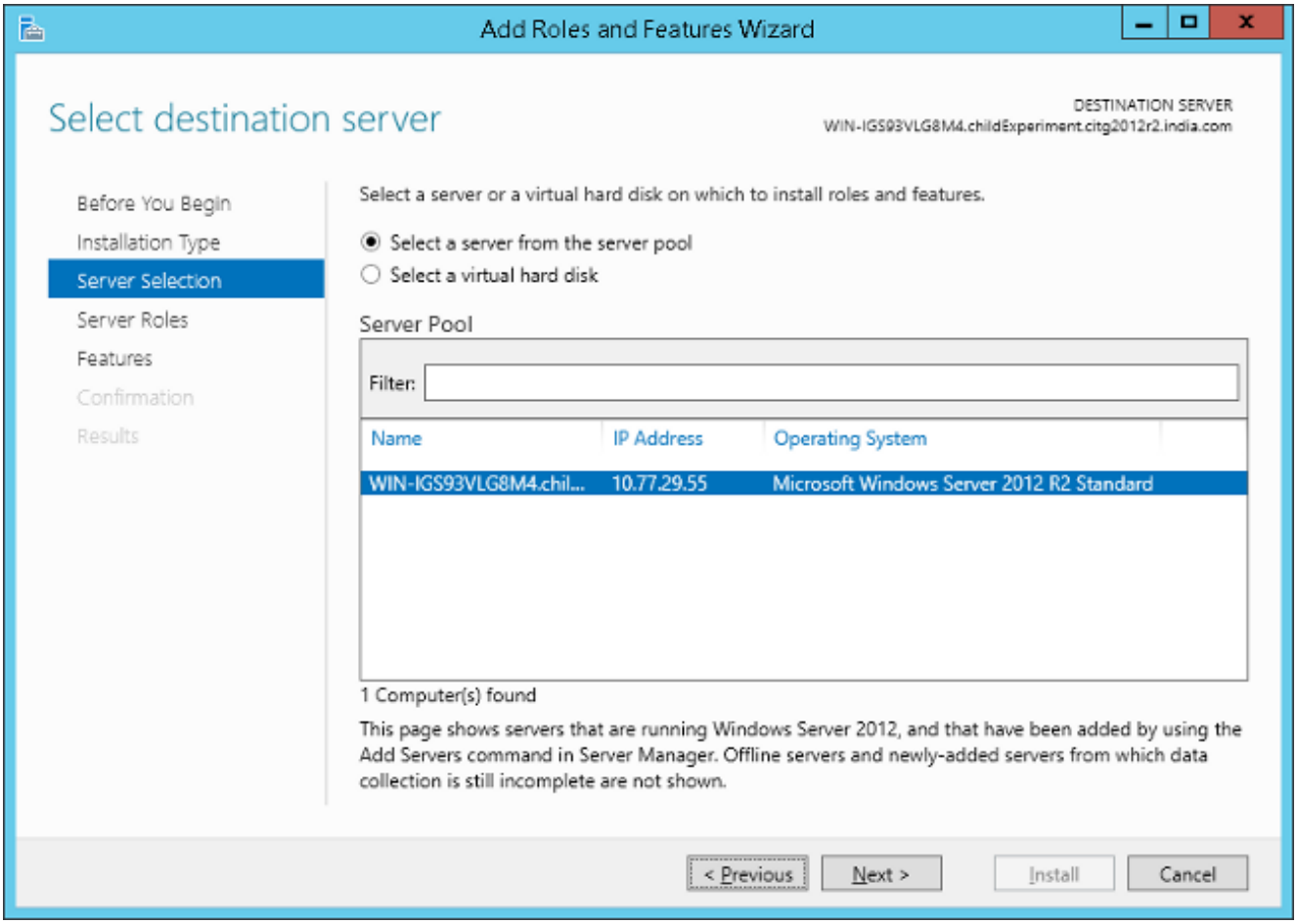
1. Open Server Manager and choose **Add Roles and Features**. Click **Next** and click **Installation Type** in order to move to the Installation Type page.



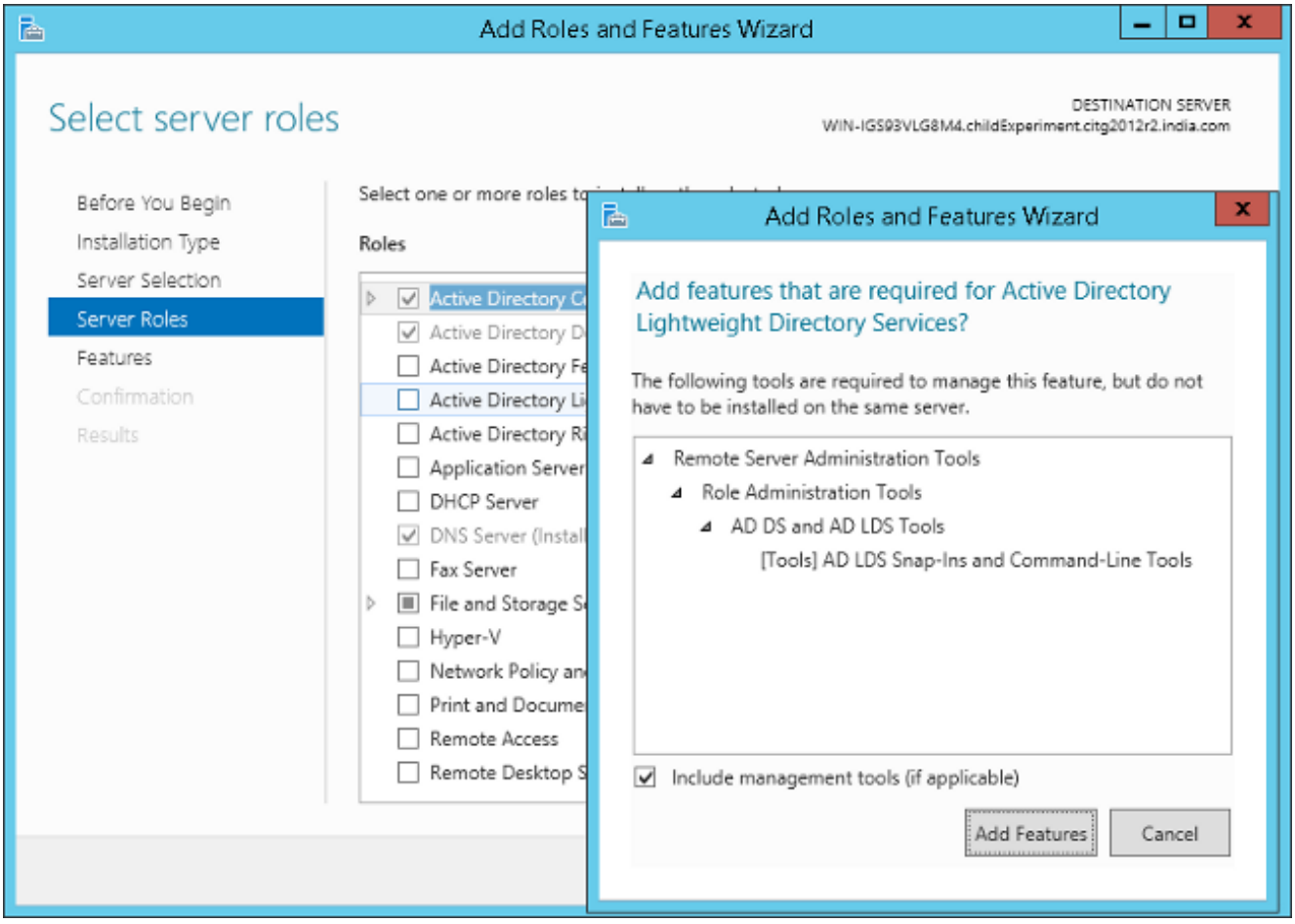
2. Choose the default options and click **Next**.



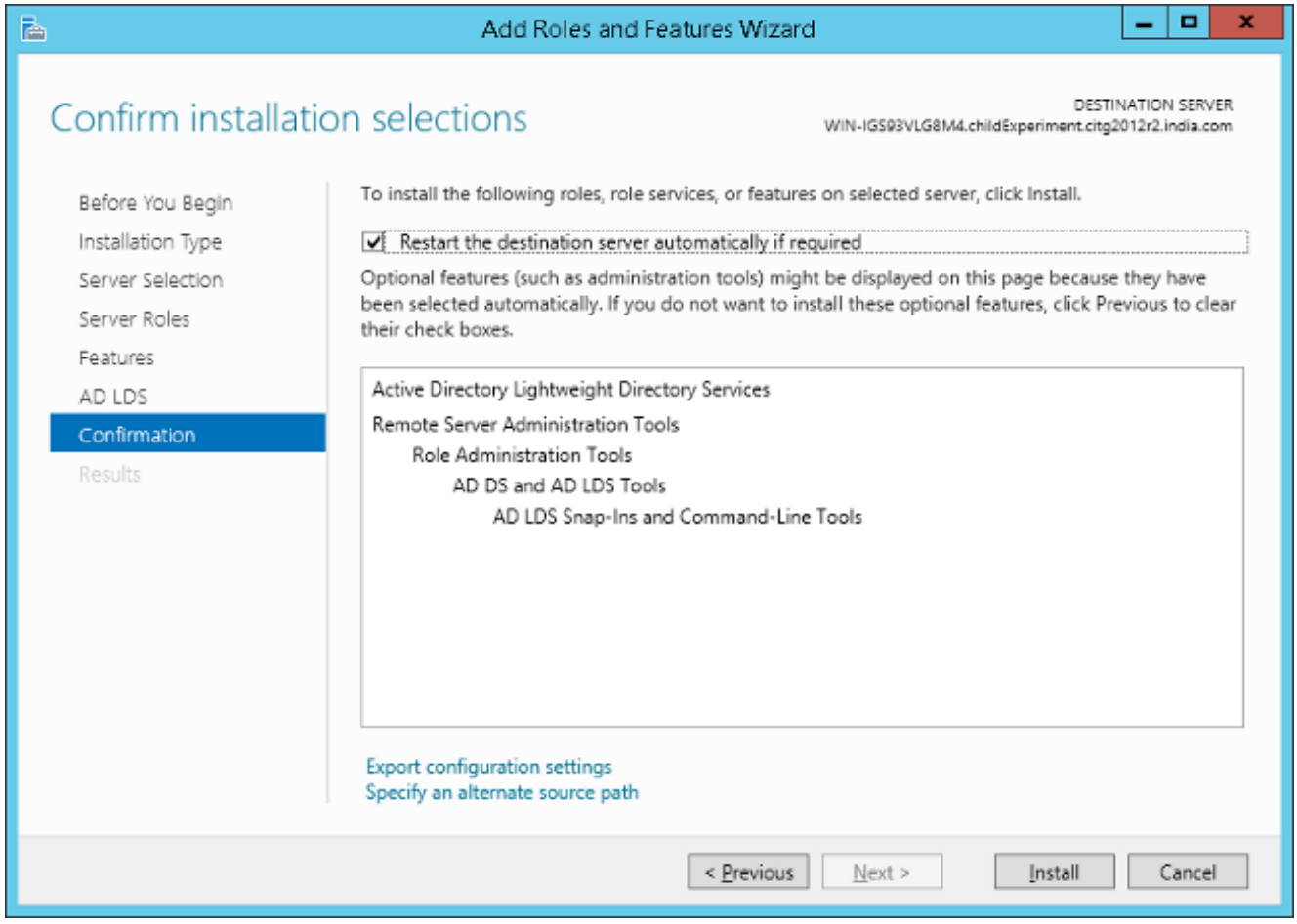
3. Click the **Select a server from the server pool** radio button in order to select the default server. Click **Next**.



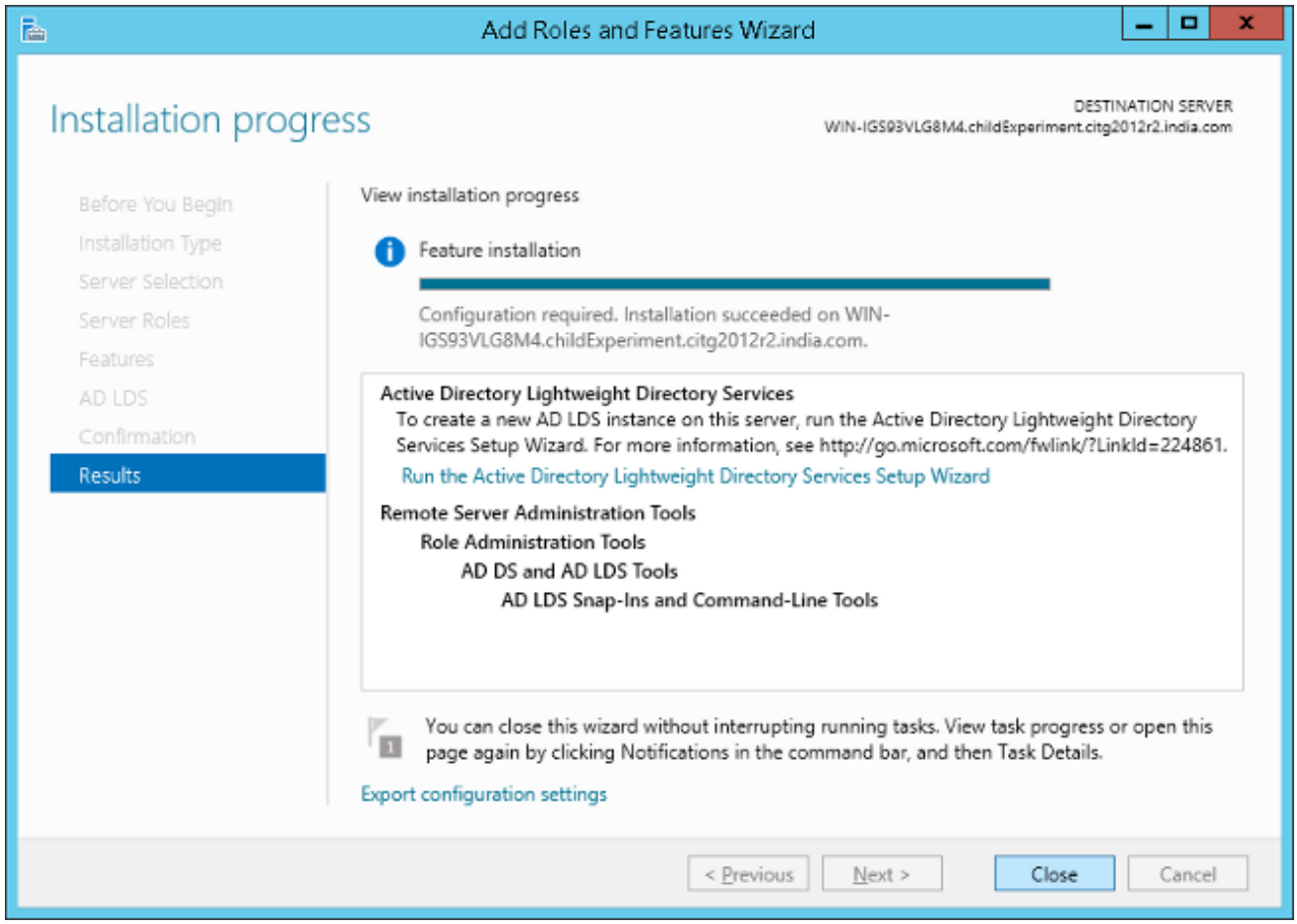
4. Check the **Active Directory Lightweight Directory Services** check box and click **Add Features**. Continue with the installation.



5. Click **Next** in the subsequent pages.
6. Click the **Restart the destination server automatically if required** checkbox and click **Install** in order to install the feature.



7. After the installation is completed successfully, click **Close** in order to close the wizard.



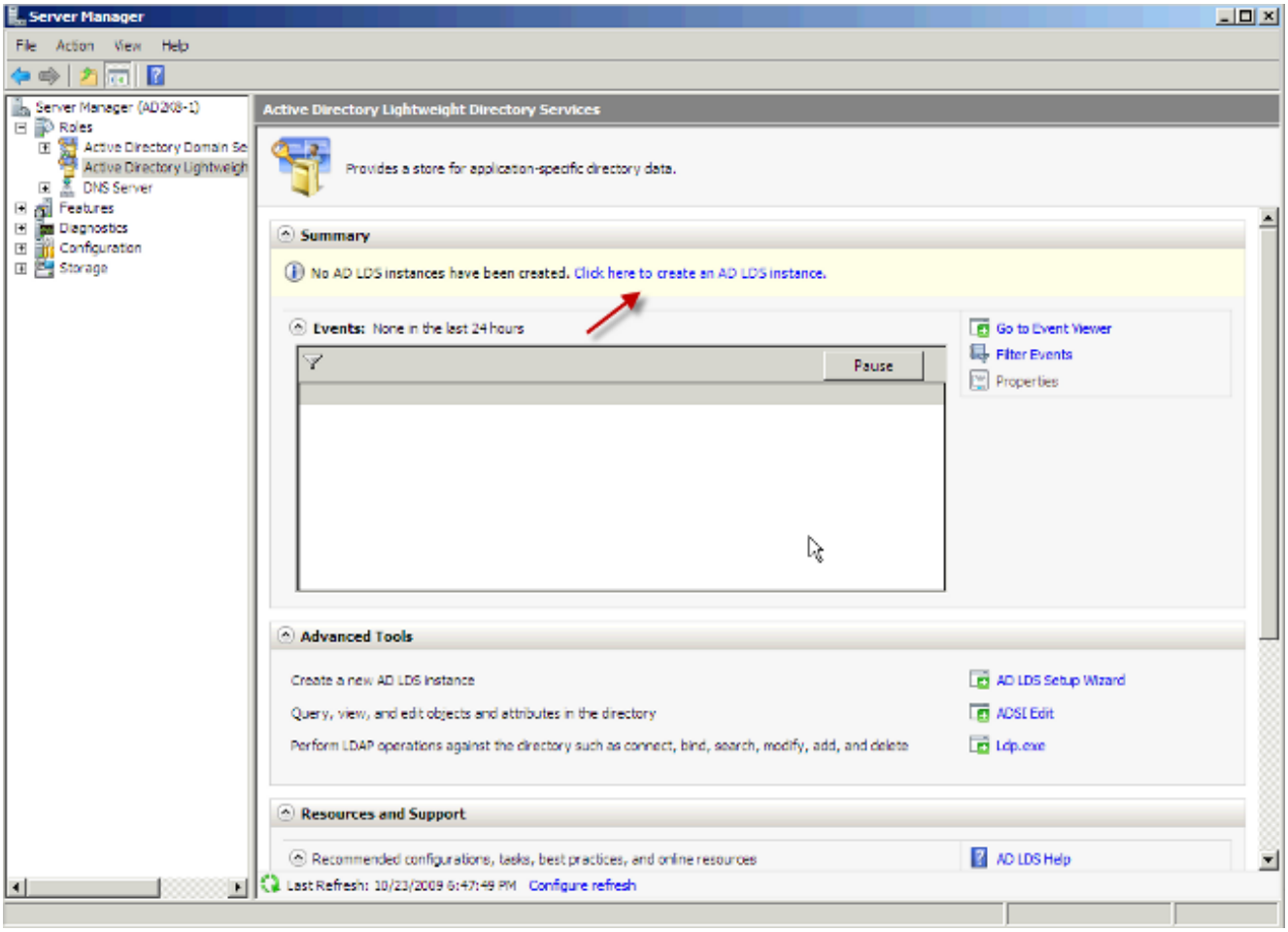
Install the Instance for Multiple Forest Support

AD LDS can run different instances of the services with different ports which allows for different user directory "applications" to be run on the same machine. By default AD LDS chooses ports 389/LDAP and 636/LDAPS, but if the system already has any kind of LDAP services that run them it will use ports 50000/LDAP and 50001/LDAPS. Each instance will have a pair of ports that increment based on the previous numbers used.

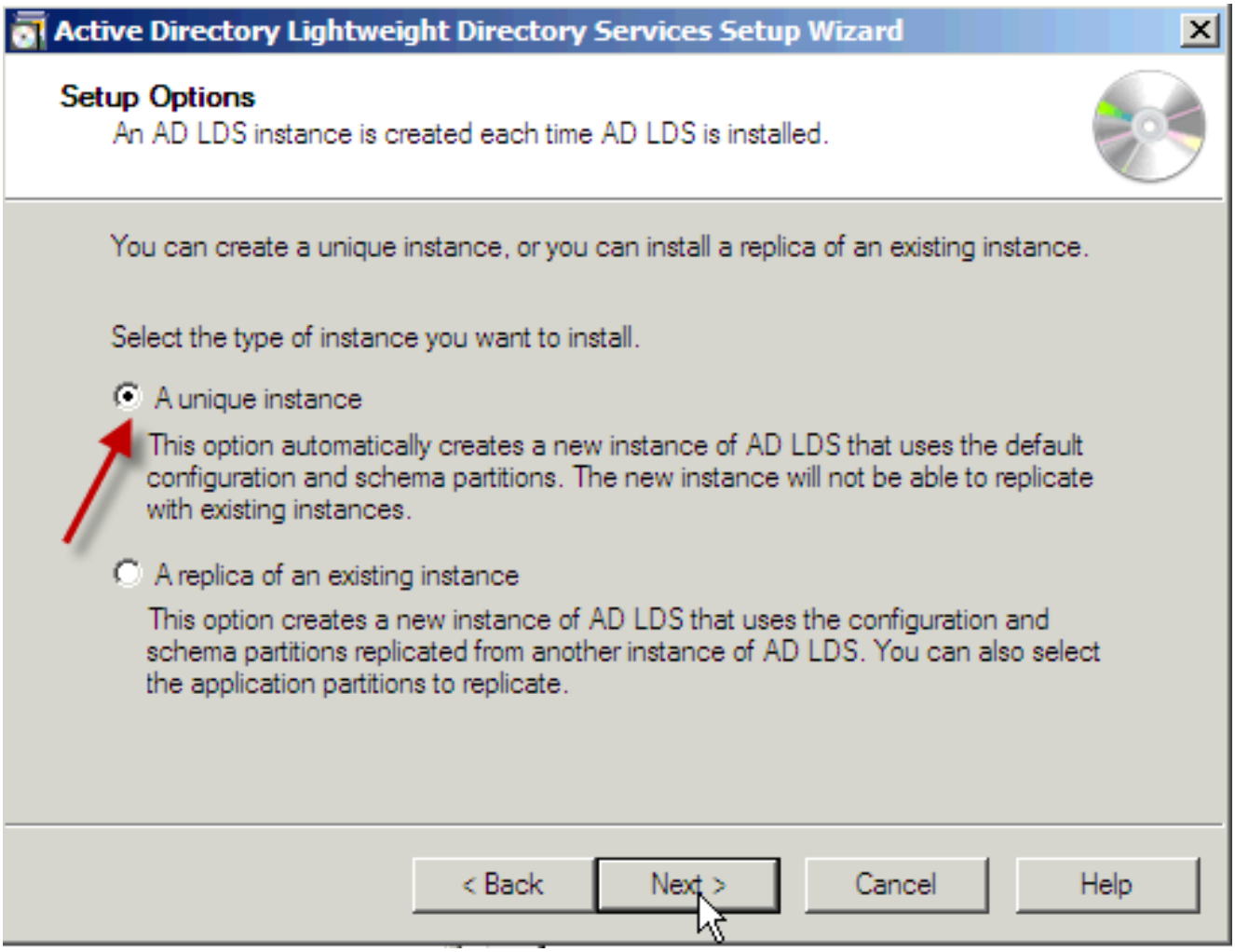
In some cases, due to a Microsoft bug, the ports are already used by the Microsoft DNS server and the instance wizard gives an error (which is not self-explanatory). This error can be fixed when you reserve the ports in the TCP/IP stack. If you find this problem, see AD LDS service start fails with error "setup could not start the service..." + error code 8007041d.

Multiple Forest Support in 2008

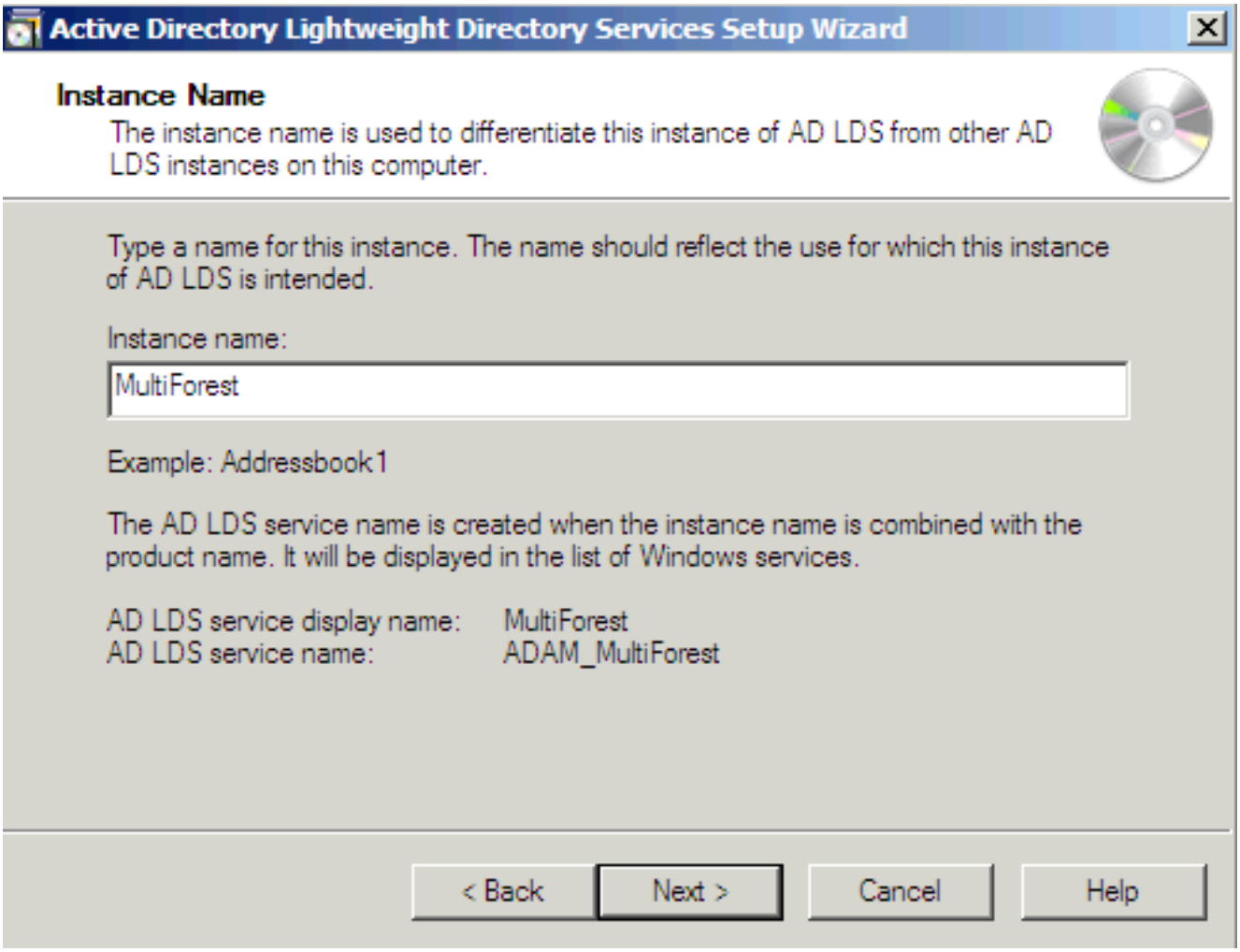
1. In the server manager, choose **Roles** and then **Active Directory Lightweight Directory Services**. Click **Click here to create an AD LDS instance**.



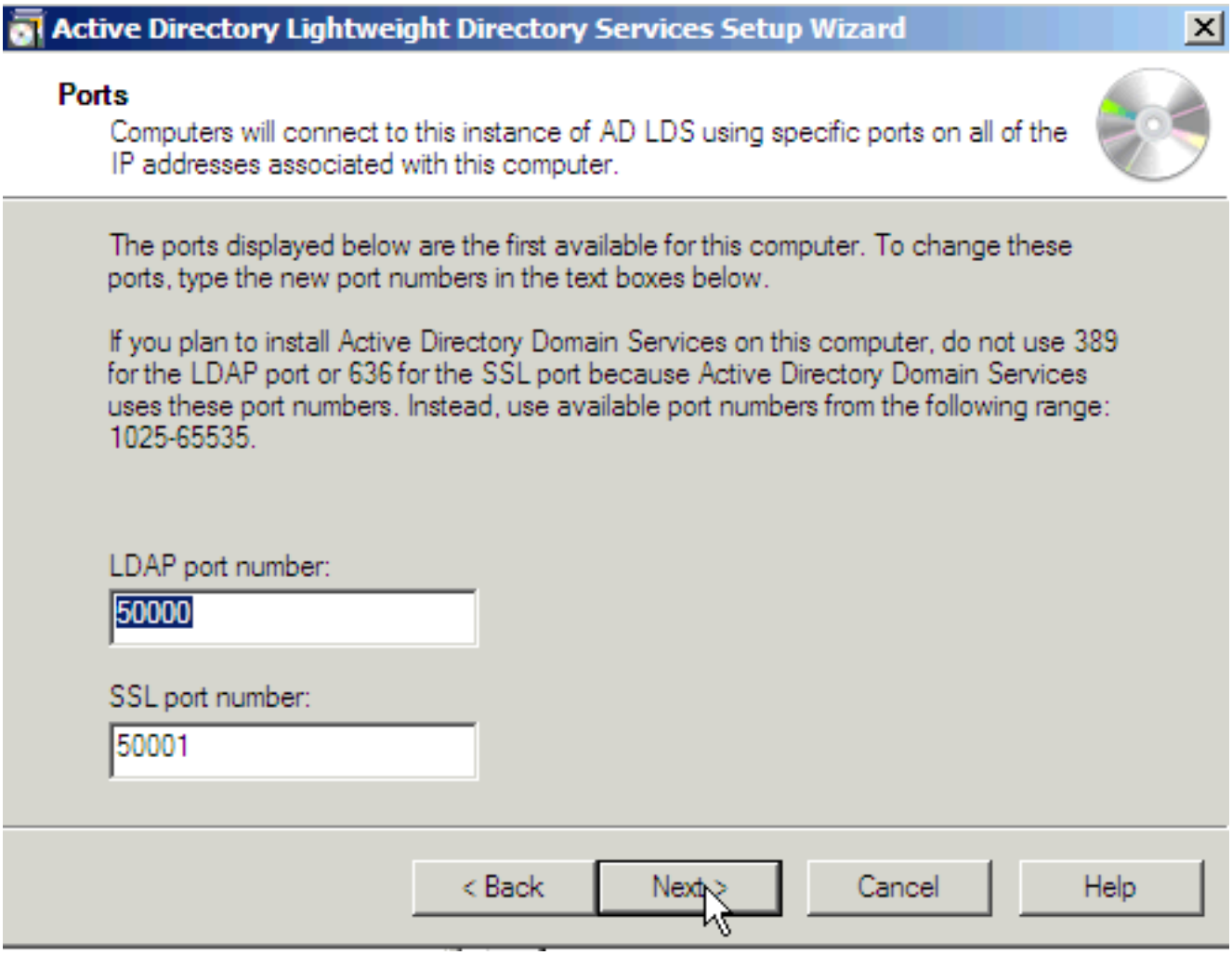
2. Click the **A unique instance** radio button. Click **Next**.



3. In the Instance name field, enter the name of the instance. It is MultiForest in this example. Click **Next**.

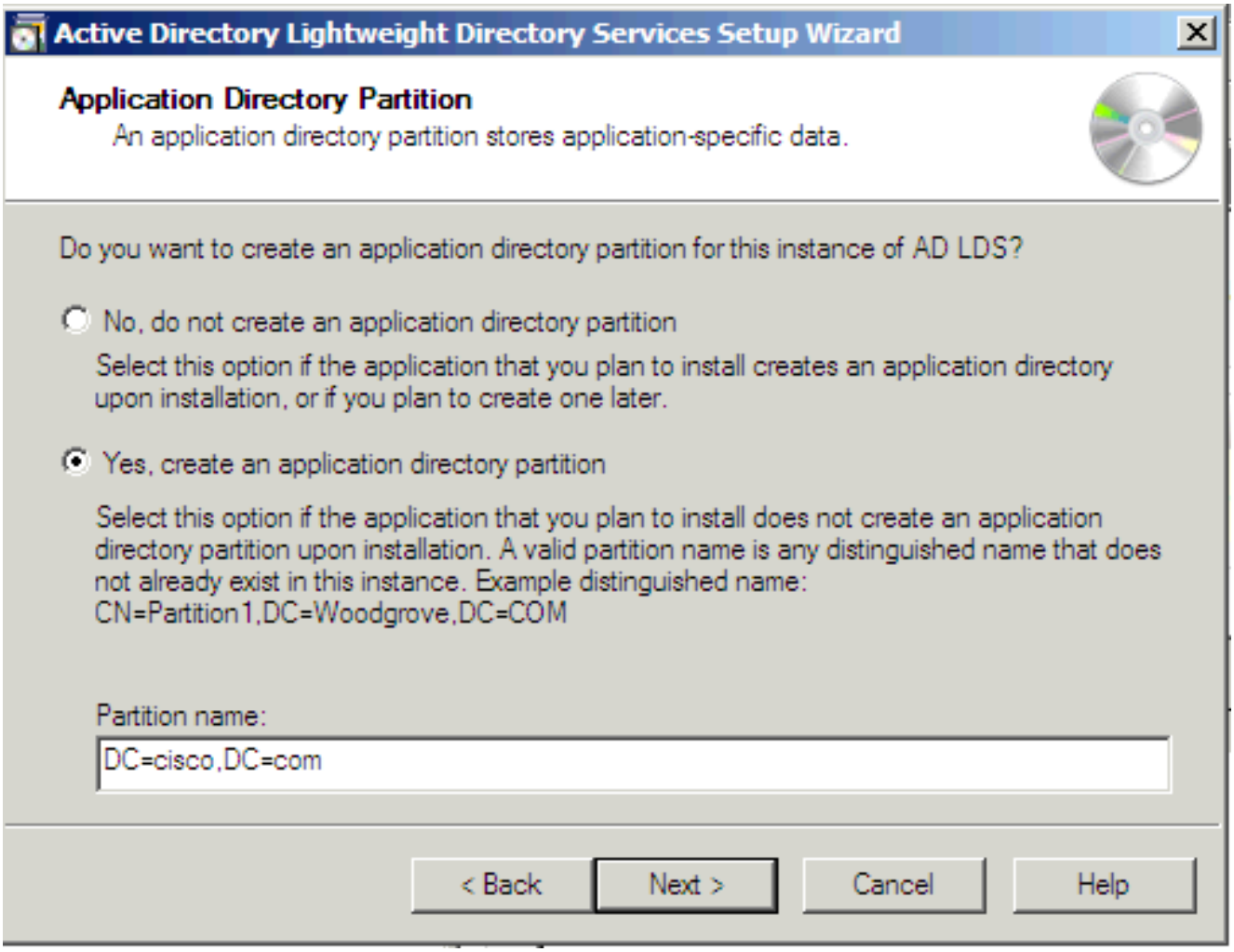


4. Enter the selected LDAP port number and SSL port number or allow the system to choose them for you. Click **Next**.

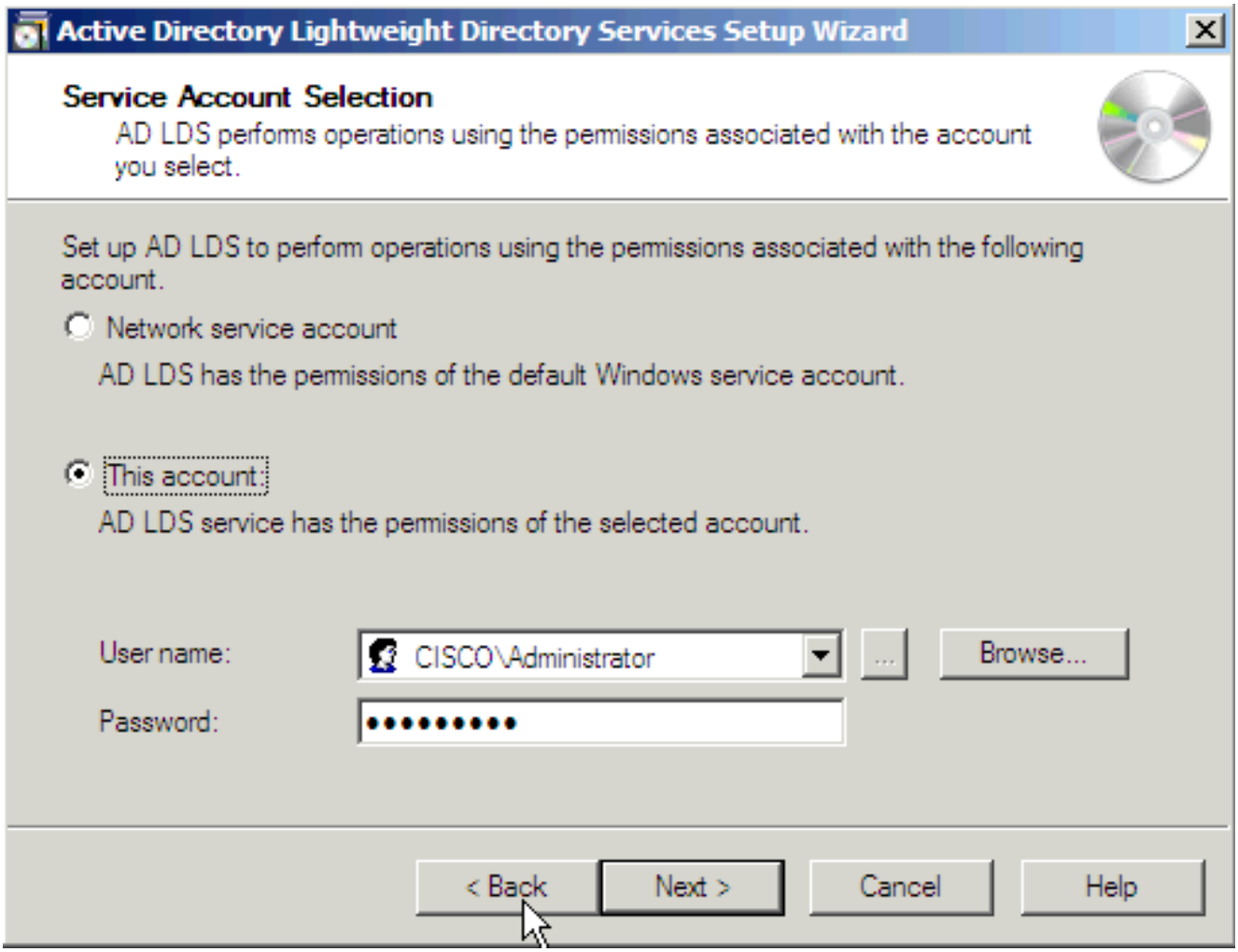


5. **Note**: CUCM supports only single application directory partition, multi partition is not supported currently.

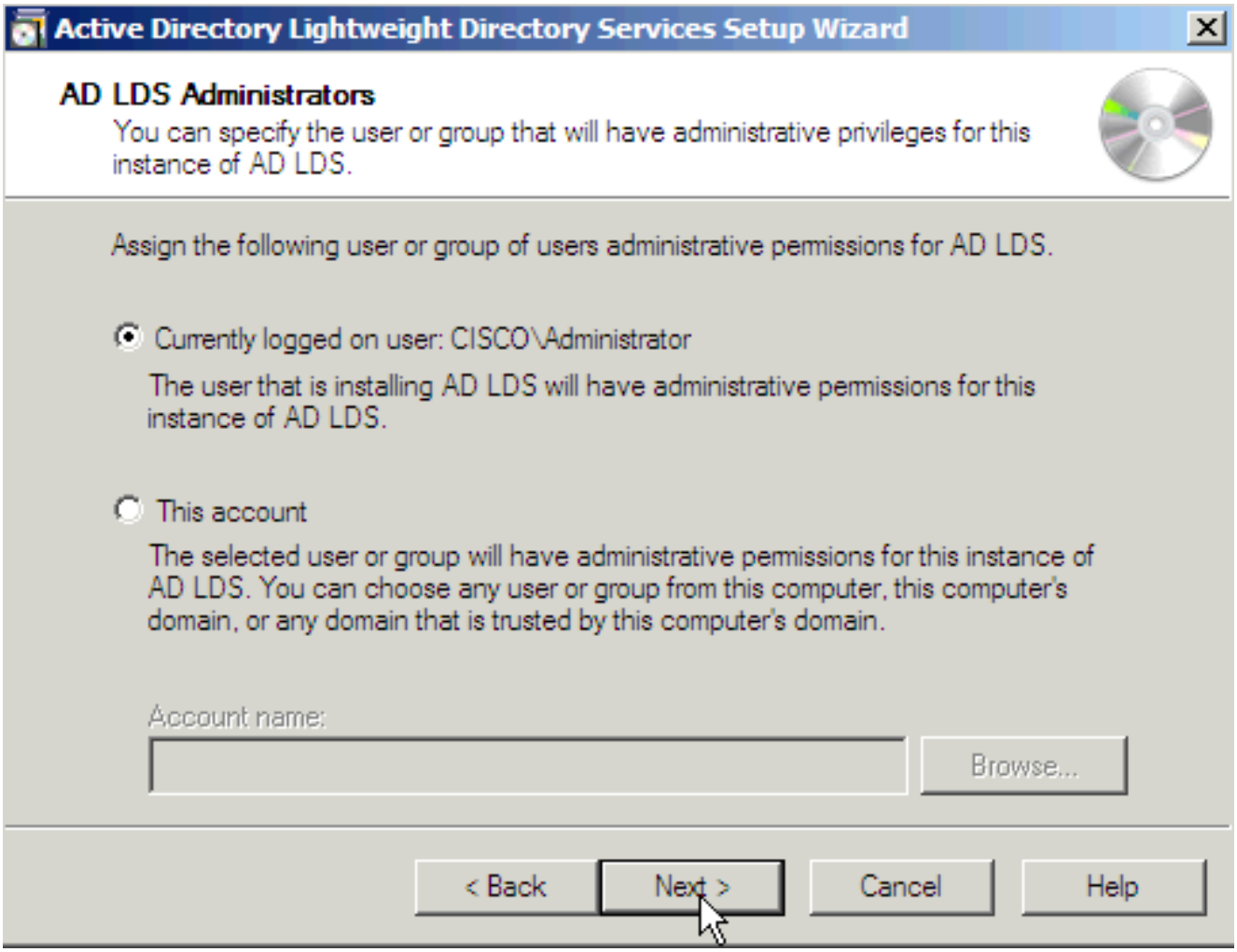
   See [Step 5: Practice Working with Application Directory Partitions] for information on how to create an Application Directory Partition. The process to create a directory partition for each domain that you want to synchronize against works based on LDAP referral (RFC 2251) and requires that the LDAP client (CUCM, CUP, and so on) supports referrals. Click the **Yes, create an application directory partition** radio button. Enter the partition name in the Partition name field for the instance. Do not provide a cn like in the example of the wizard, because most of the time that creates an error in the Schemas. In this scenario, the same partition as the AD domain controller that hosts AD LDS (dc=Cisco,dc=com) was entered. Click
   Next.



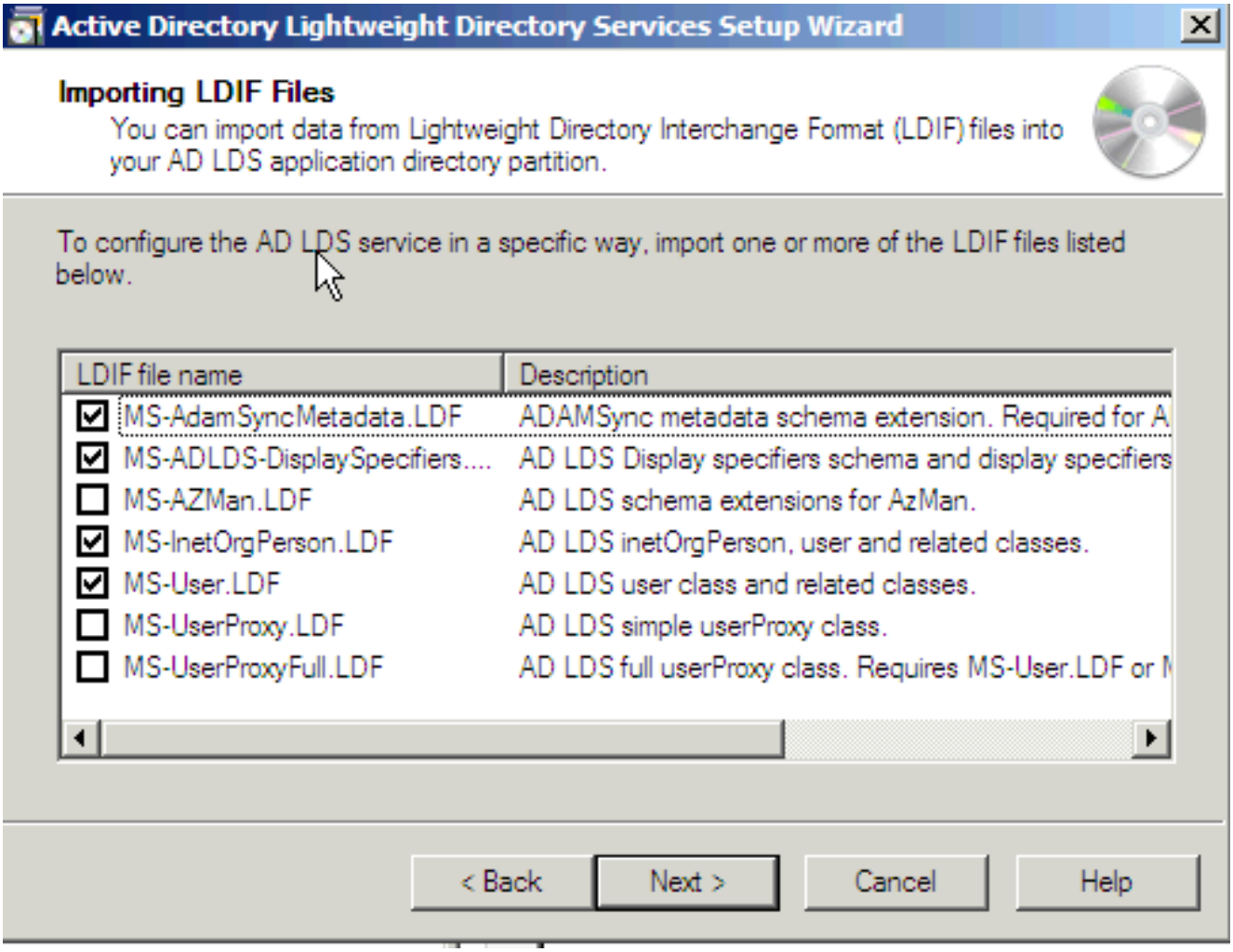
6. Click the **This account** radio button. Enter a User name and Password in order to start the server. Click **Next**.



7. Click the **Currently logged on user** radio button. Enter the name of the user with administrative permissions. Click **Next**.



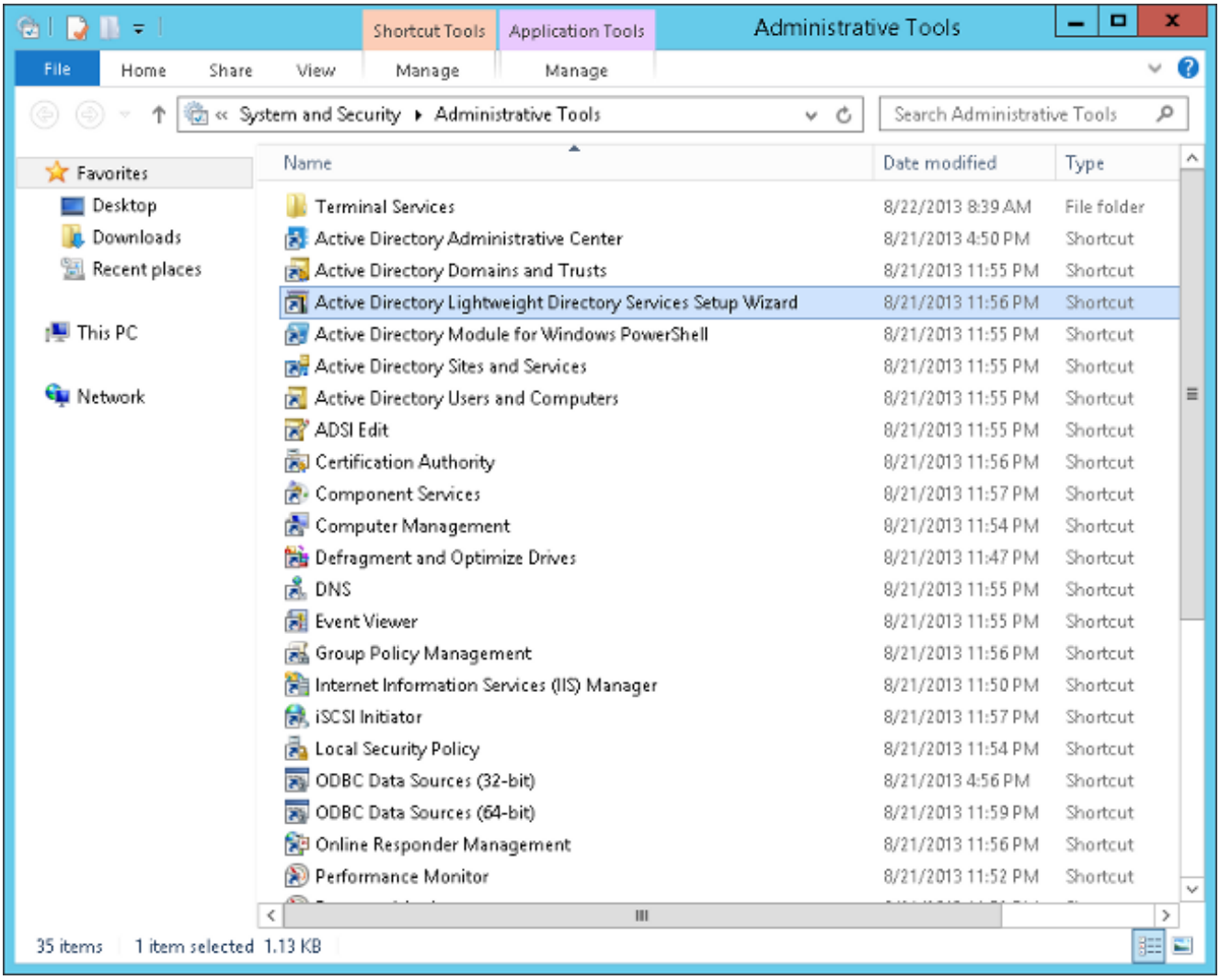
8. Import the highlighted default LDIF files in order to build the schema. Click **Next**.



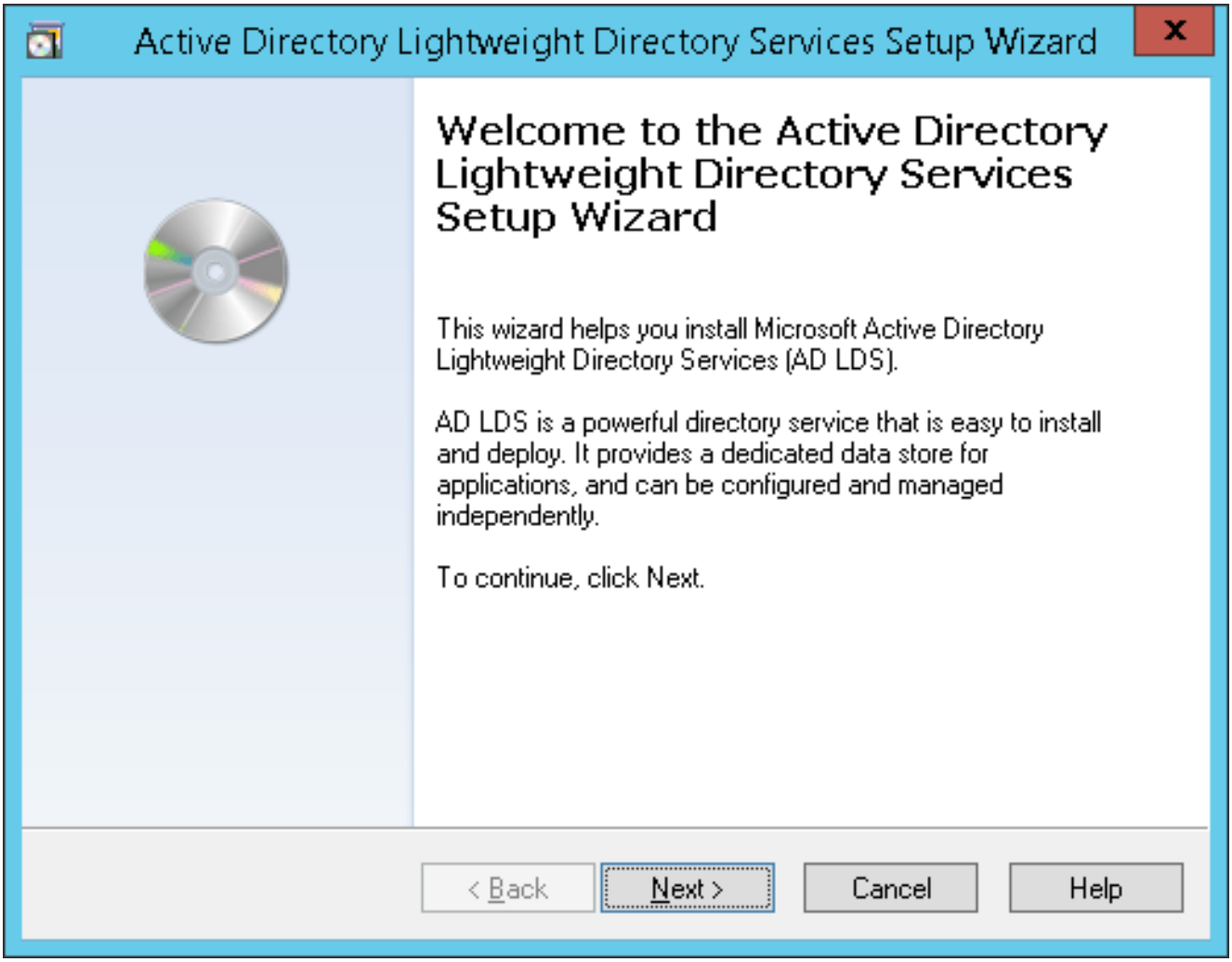
Note: If ADAM is installed on a Windows 2003 sever, then the previous screen will have only four options: MS-AZMan.LDF, MS-InetOrgPerson.LDF, MS-User.LDF, and MS-UserProxy.LDF. From these four, check only the check boxes for MS-User.LDF and MS-InetOrgPerson.LDF.

Multiple Forest Support in 2012

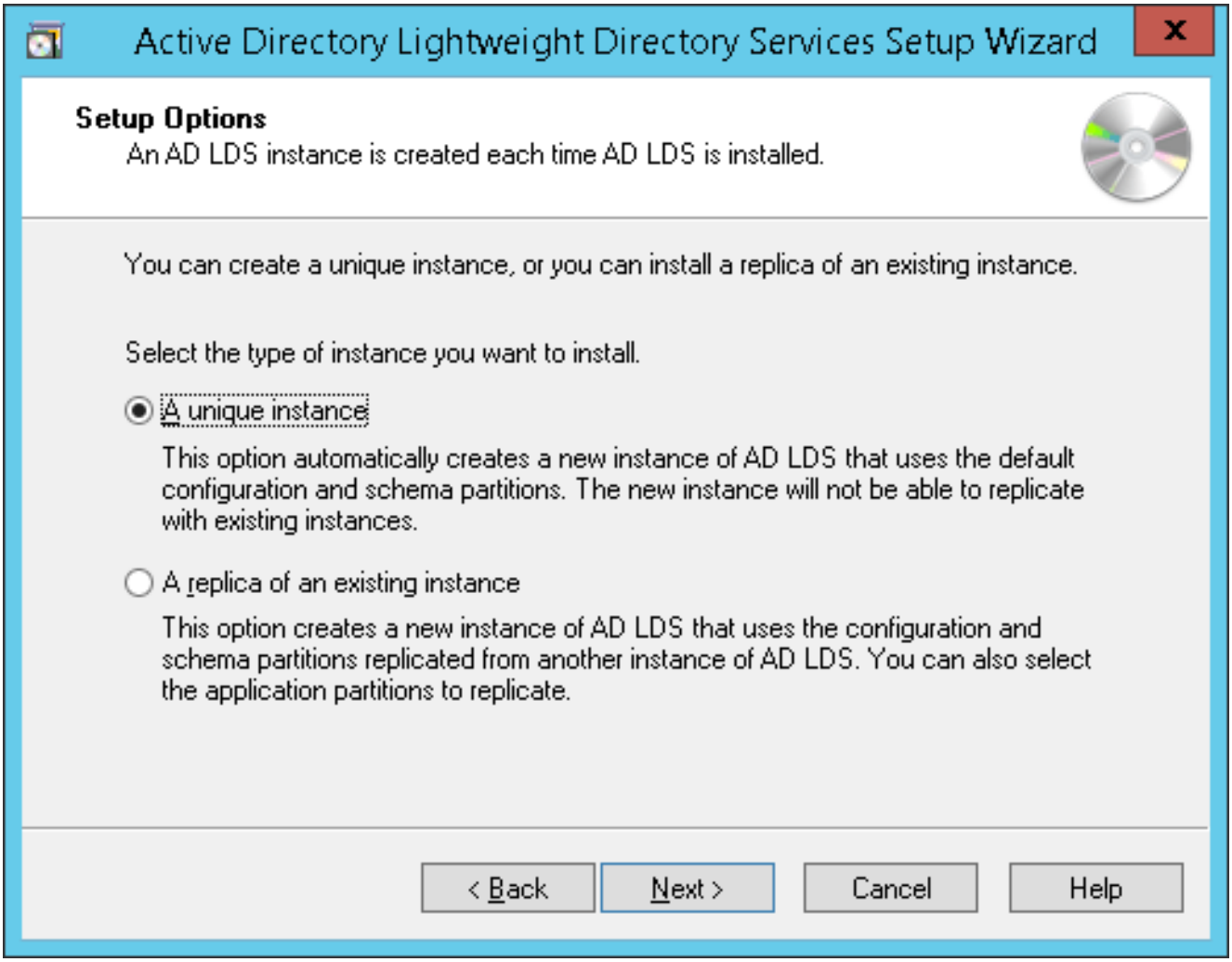
1. Open the Administrative tools and double-click **Active Directory Lightweight Directory Services Setup Wizard**.


Shortcut Tools
Application Tools
Administrative Tools
File
Home
Share
View
Manage
Manage
System and Security ▸ Administrative Tools
Search Administrative Tools
Favorites
Desktop
Downloads
Recent places
This PC
Network
Name
Date modified
Type
Terminal Services 8/22/2013 8:39 AM File folder
Active Directory Administrative Center 8/21/2013 4:50 PM Shortcut
Active Directory Domains and Trusts 8/21/2013 11:55 PM Shortcut
Active Directory Lightweight Directory Services Setup Wizard 8/21/2013 11:56 PM Shortcut
Active Directory Module for Windows PowerShell 8/21/2013 11:55 PM Shortcut
Active Directory Sites and Services 8/21/2013 11:55 PM Shortcut
Active Directory Users and Computers 8/21/2013 11:55 PM Shortcut
ADSI Edit 8/21/2013 11:55 PM Shortcut
Certification Authority 8/21/2013 11:56 PM Shortcut
Component Services 8/21/2013 11:57 PM Shortcut
Computer Management 8/21/2013 11:54 PM Shortcut
Defragment and Optimize Drives 8/21/2013 11:47 PM Shortcut
DNS 8/21/2013 11:55 PM Shortcut
Event Viewer 8/21/2013 11:55 PM Shortcut
Group Policy Management 8/21/2013 11:56 PM Shortcut
Internet Information Services (IIS) Manager 8/21/2013 11:50 PM Shortcut
iSCSI Initiator 8/21/2013 11:57 PM Shortcut
Local Security Policy 8/21/2013 11:54 PM Shortcut
ODBC Data Sources (32-bit) 8/21/2013 4:56 PM Shortcut
ODBC Data Sources (64-bit) 8/21/2013 11:59 PM Shortcut
Online Responder Management 8/21/2013 11:56 PM Shortcut
Performance Monitor 8/21/2013 11:52 PM Shortcut
35 items
1 item selected 1.13 KB

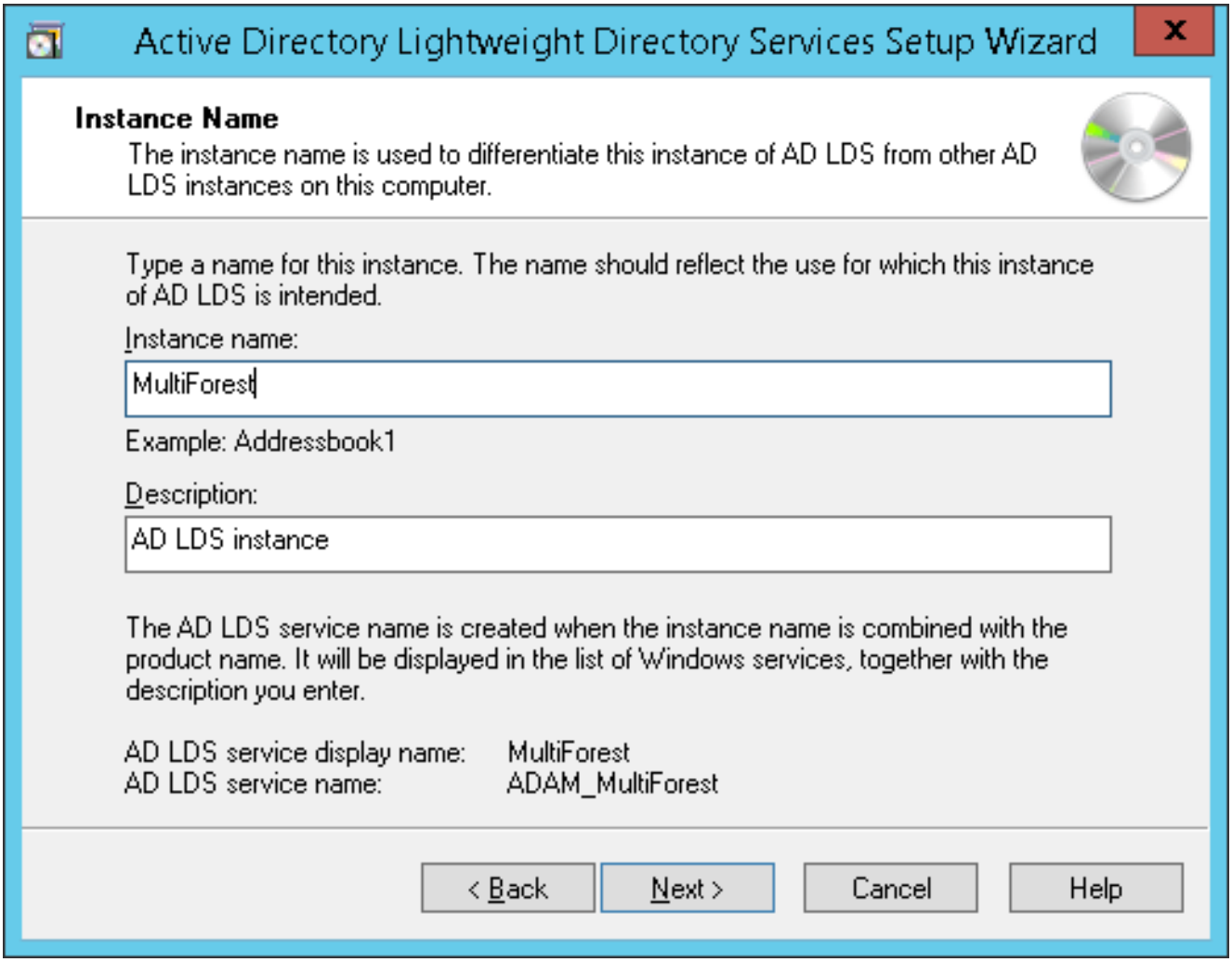
2. Click **Next**.



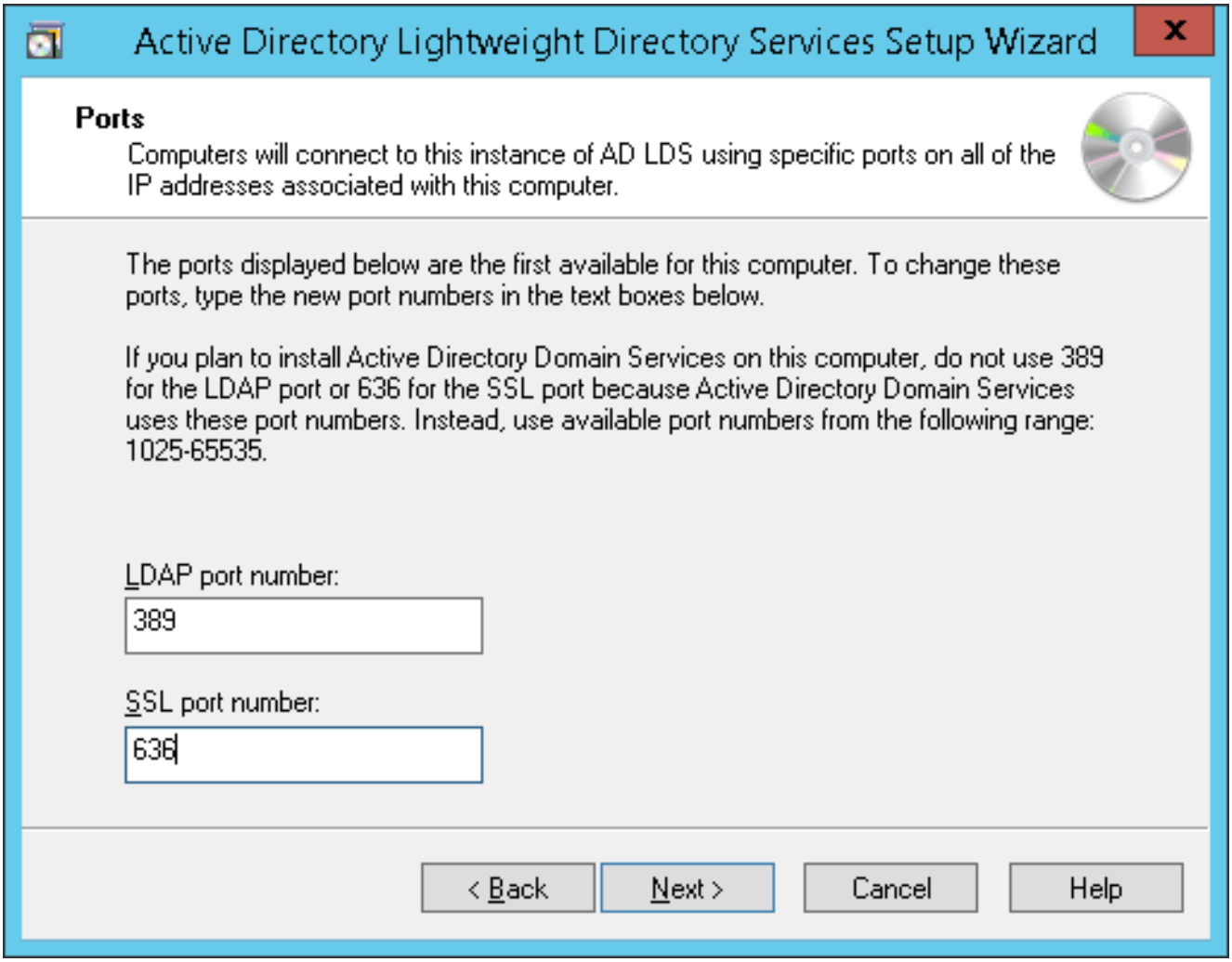
3. Check the **A unique instance** radio button. Click **Next**.



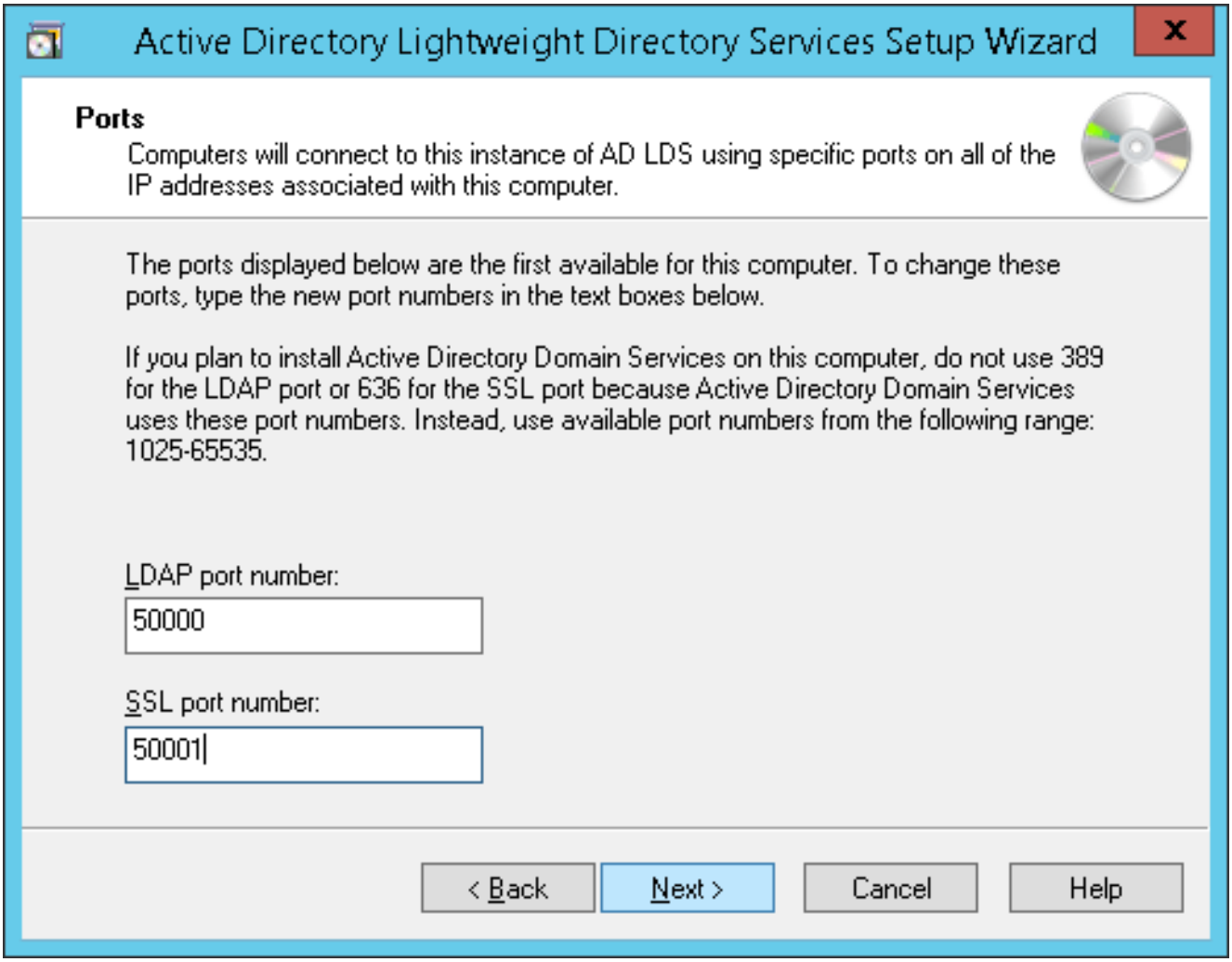
4. Enter an Instance Name and Description for the instance. The name "MultiForest" is entered here. Click **Next**.



5. Enter the LDAP and SSL port numbers. The preferred ports are 389 and 636 respectively. If the domain server is a child server and if the parent domain uses these ports, then by default different port numbers will be populated. In that case, do not change them and continue with the installation. Click **Next**.

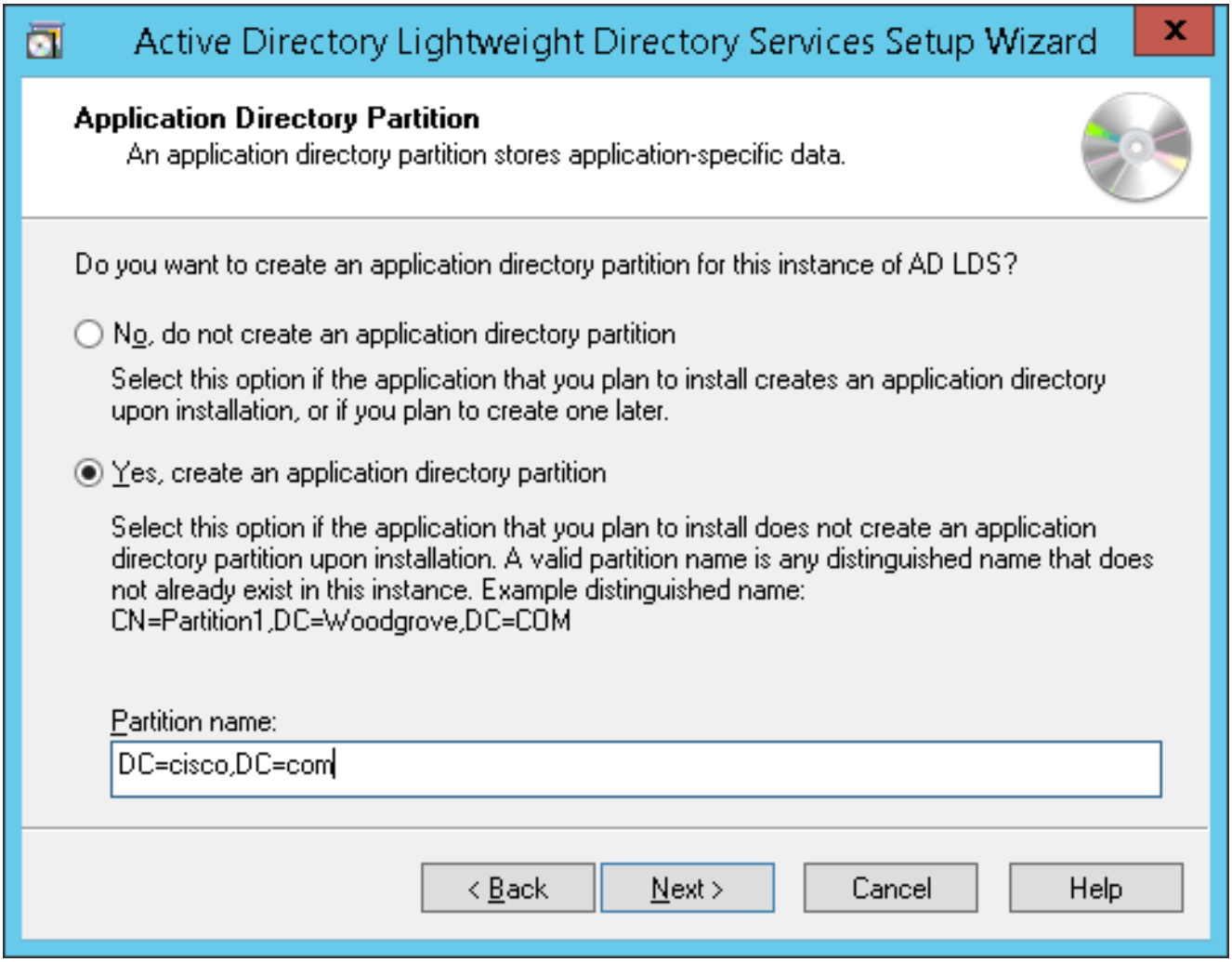


6. Here, by default, other port numbers have been populated. Click **Next**.

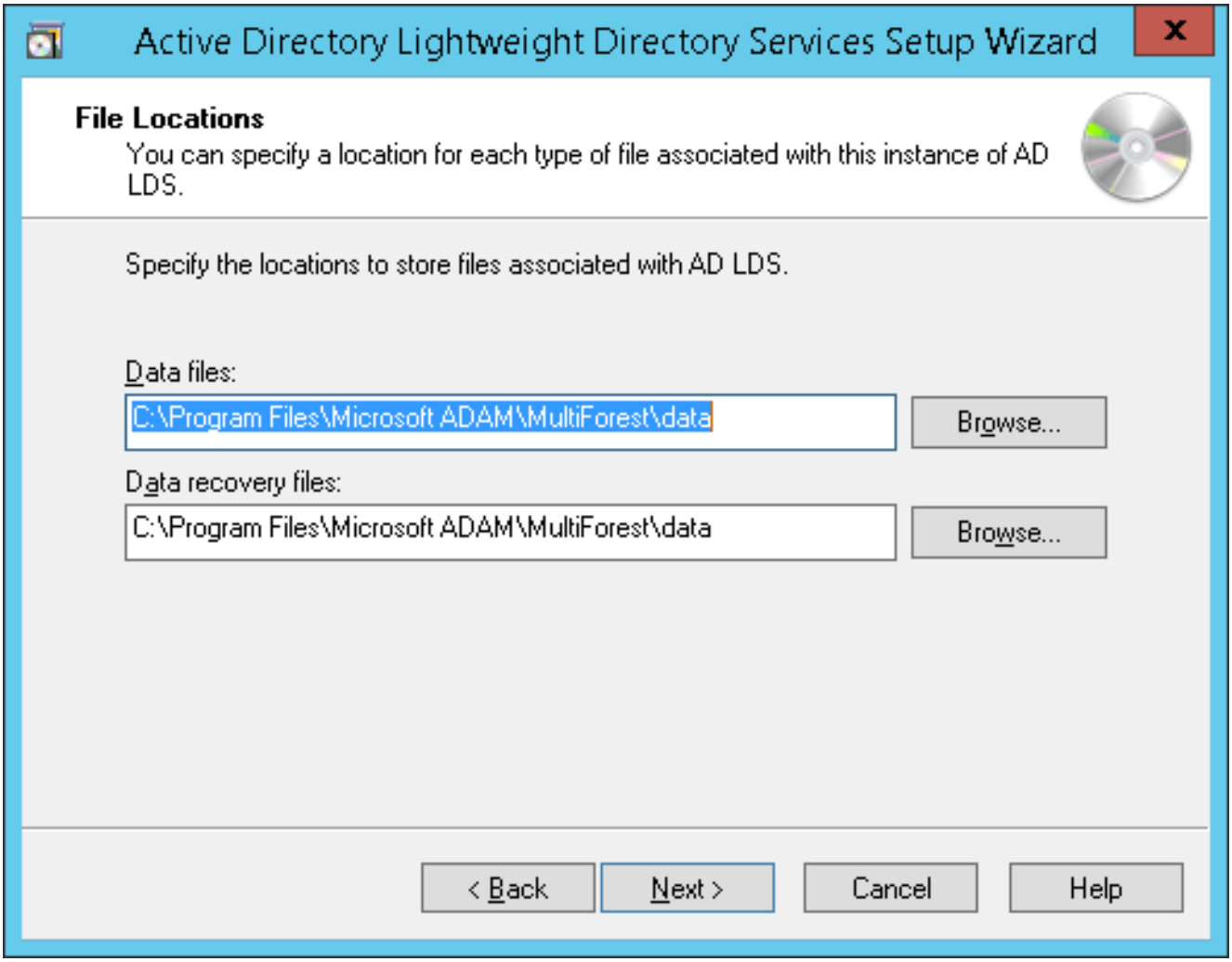


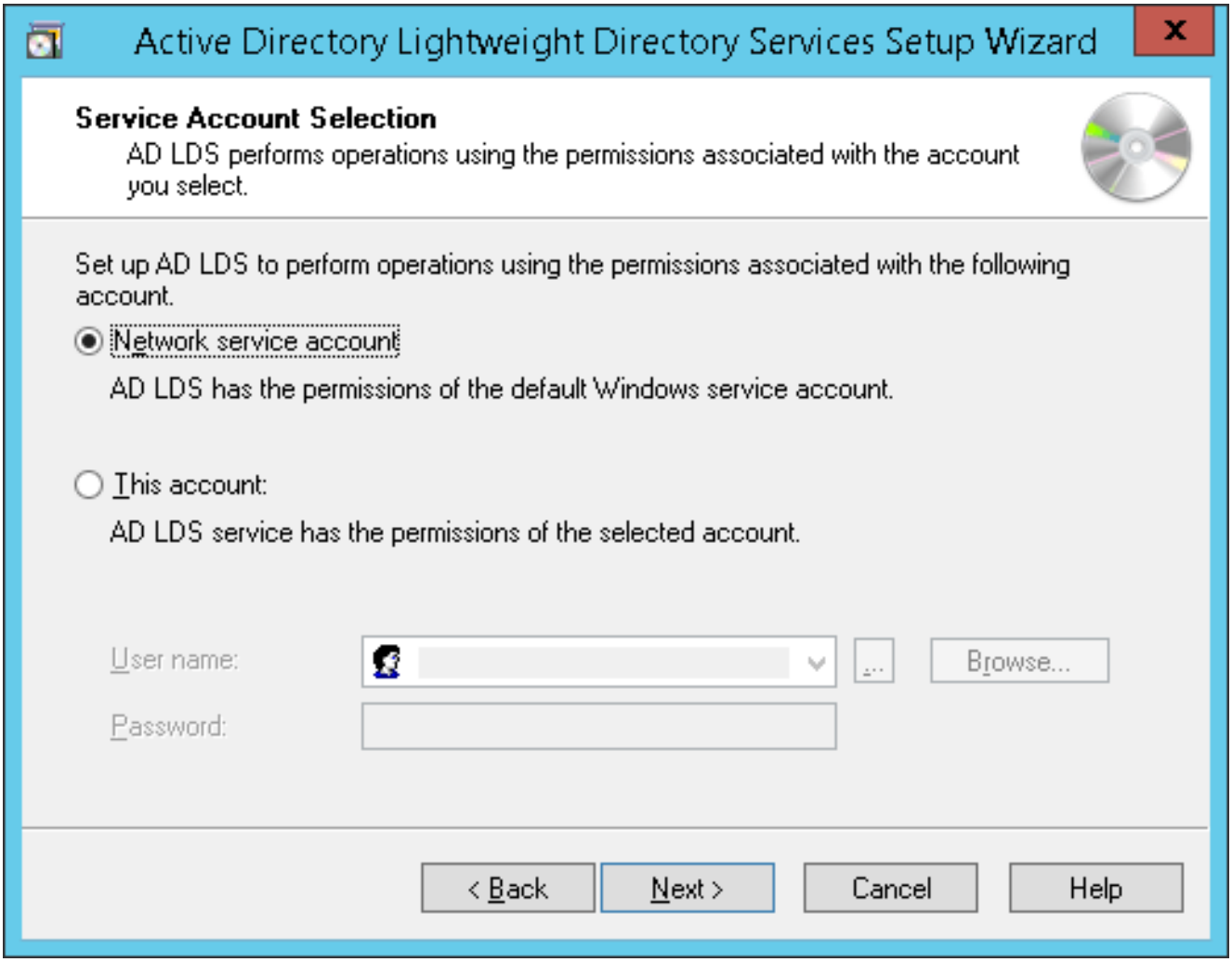
7. **Note**: CUCM supports only single application directory partition, multi partition is not supported currently.

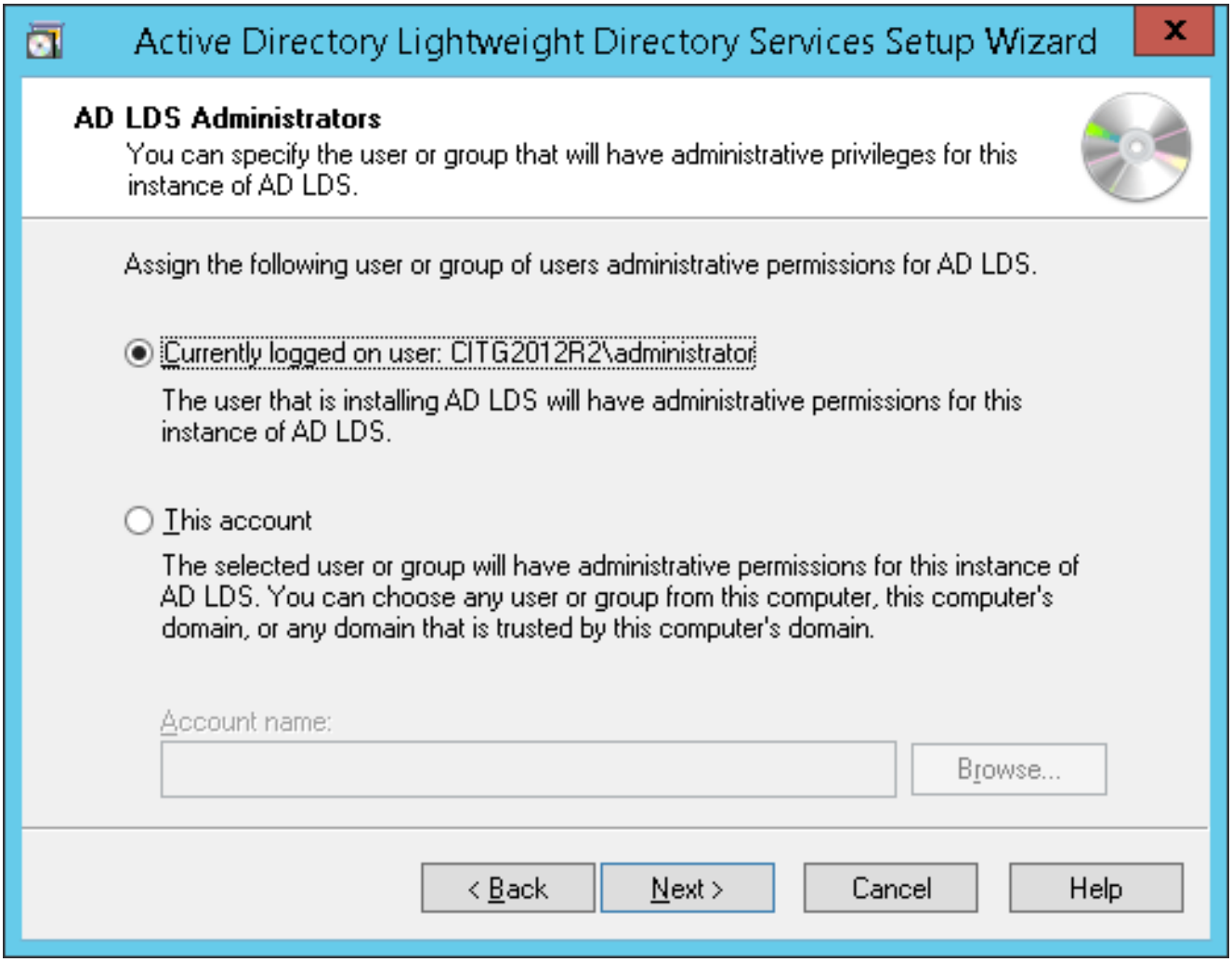
   See Step 5: Practice Working with Application Directory Partitions for information on how to create an Application Directory Partition. The process to create a directory partition for each domain that you want to synchronize against works based on LDAP referral (RFC 2251) and requires that the LDAP client (CUCM, CUP, and so on) supports referrals. See Microsoft Support for more information. Click the **Yes, create an application directory partition** radio button. Enter the Partition Name. Create the partition for LDS as cisco.com. Any suitable value can be provided. Click
   Next.



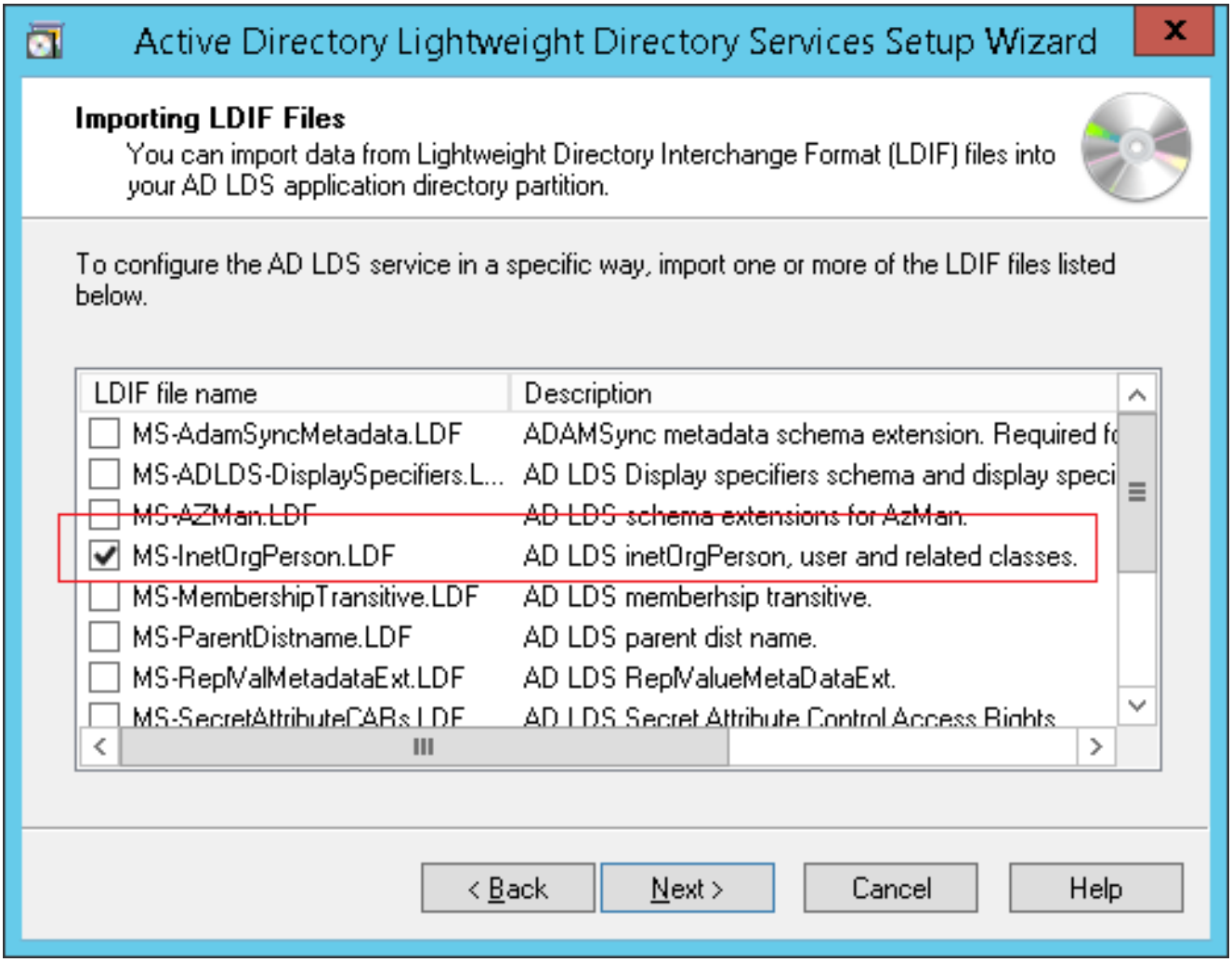
8. Choose the default options in subsequent pages and continue.

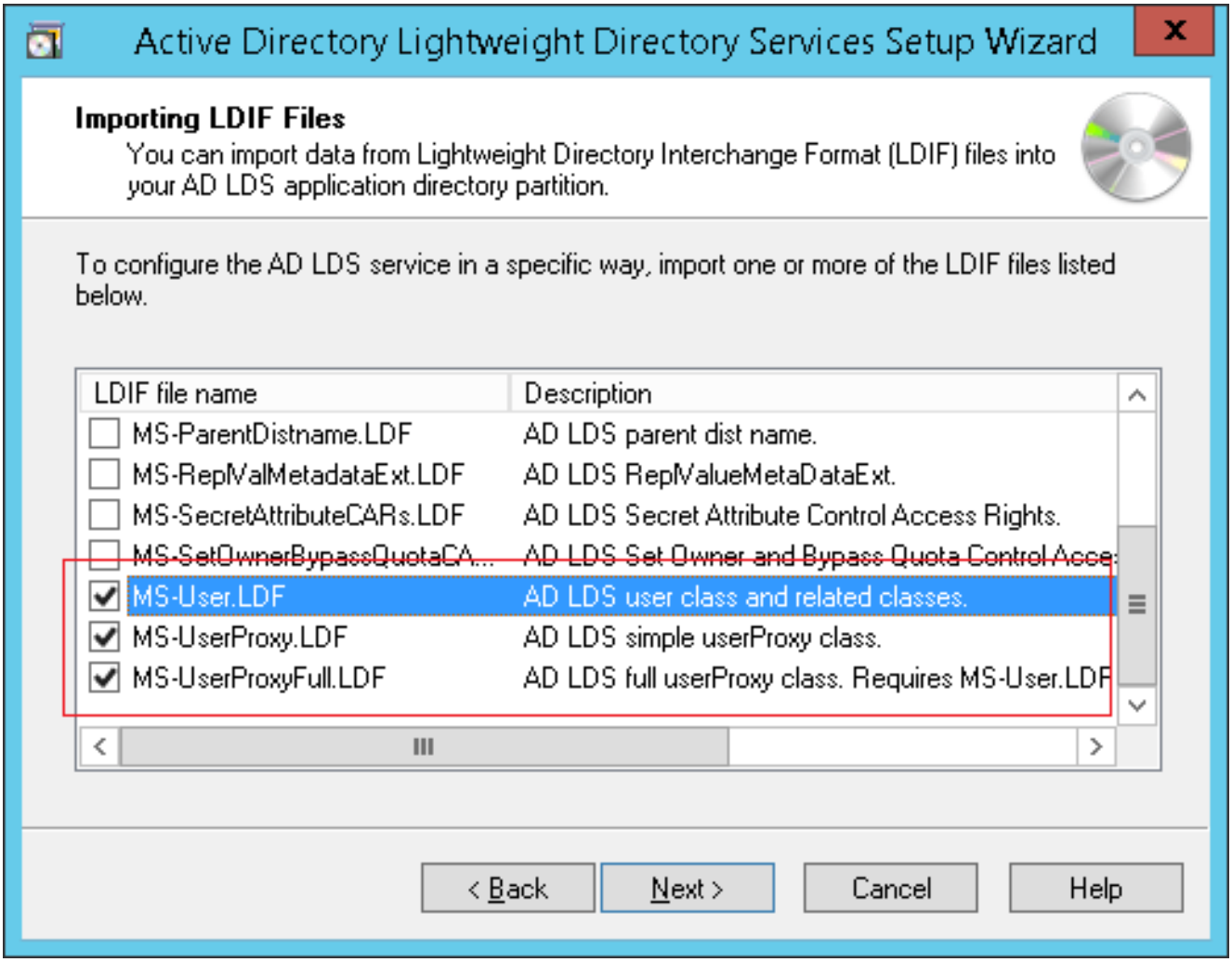

Active Directory Lightweight Directory Services Setup Wizard
File Locations
You can specify a location for each type of file associated with this instance of AD LDS.
Specify the locations to store files associated with AD LDS.
Data files:
C:\Program Files\Microsoft ADAM\MultiForest\data
Browse...
Data recovery files:
C:\Program Files\Microsoft ADAM\MultiForest\data
Browse...
< Back
Next >
Cancel
Help


Active Directory Lightweight Directory Services Setup Wizard
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:
...
Browse...
Password:
< Back
Next >
Cancel
Help

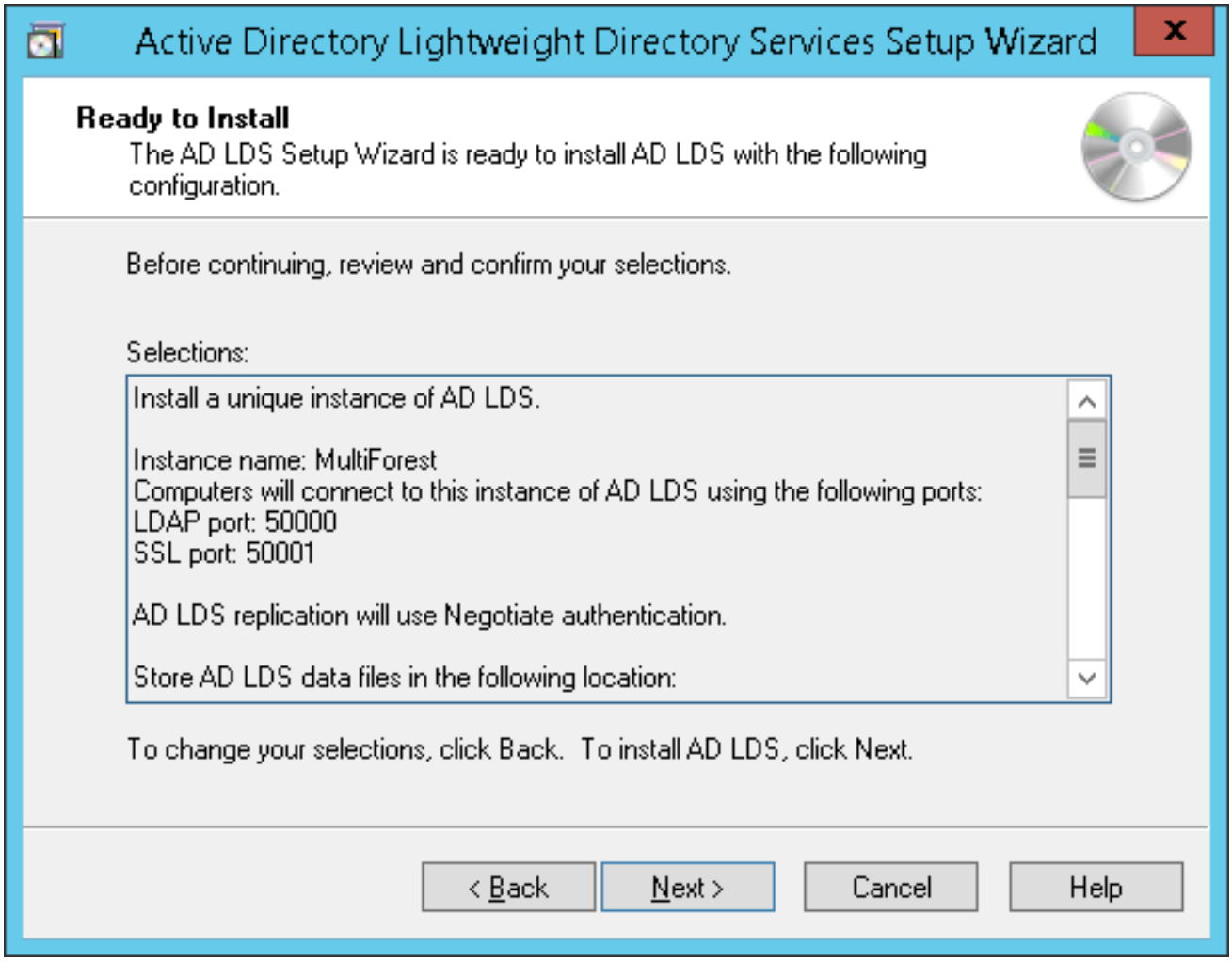


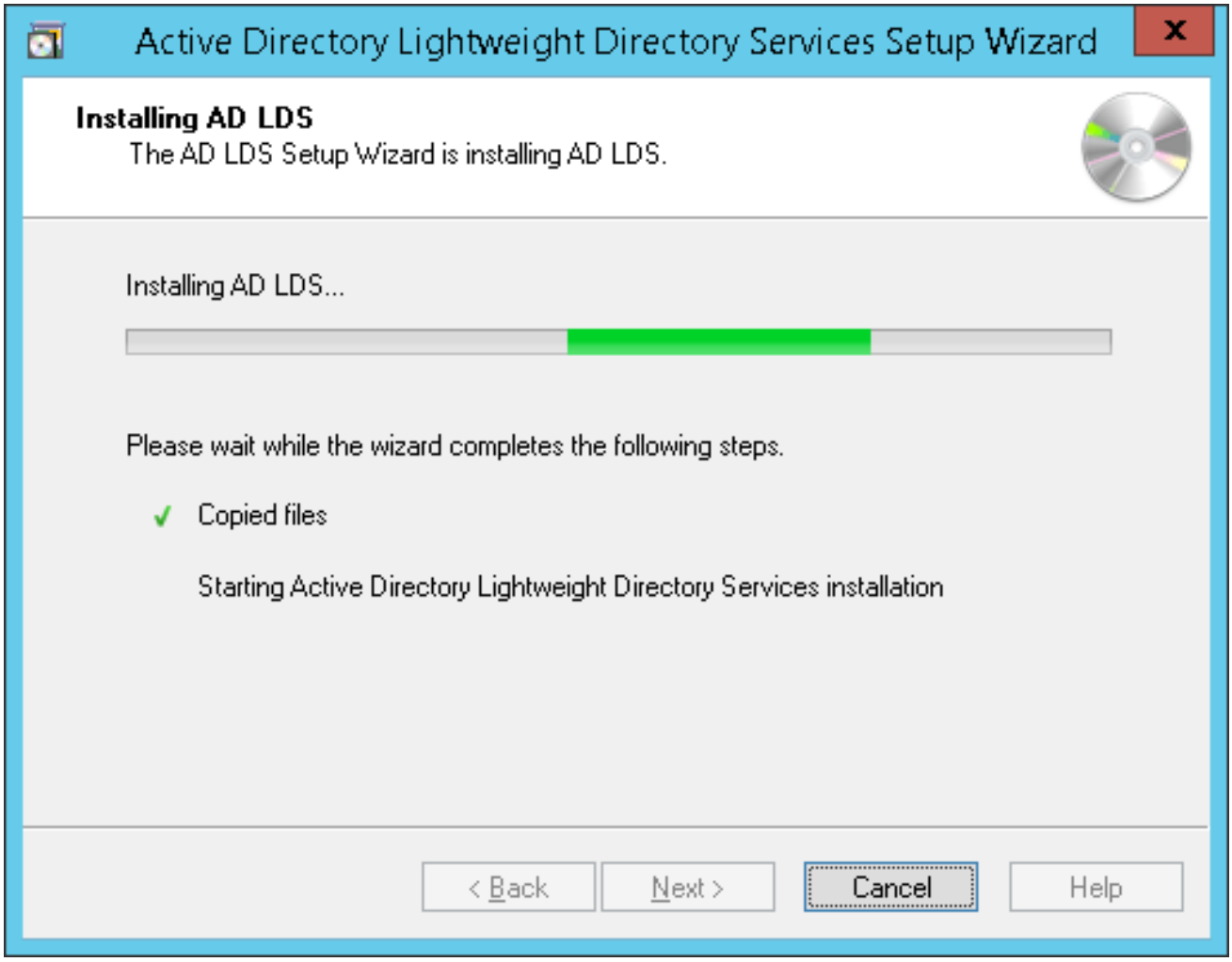
9. Check the **MS-InetOrgPerson.LDF**, **MS-User.LDF**, **MS-UserProxy.LDF**, and **MS-UserProxyFull.LDF** check boxes. Click **Next**.


Active Directory Lightweight Directory Services Setup Wizard
Importing LDIF Files
You can import data from Lightweight Directory Interchange Format (LDIF) files into your AD LDS application directory partition.
To configure the AD LDS service in a specific way, import one or more of the LDIF files listed below.
LDIF file name
Description
MS-AdamSyncMetadata.LDF
ADAMSync metadata schema extension. Required f
MS-ADLDS-DisplaySpecifiers.L...
AD LDS Display specifiers schema and display speci
MS-AZMan.LDF
AD LDS schema extensions for AzMan.
MS-InetOrgPerson.LDF
AD LDS inetOrgPerson, user and related classes.
MS-MembershipTransitive.LDF
AD LDS memberhsip transitive.
MS-ParentDistname.LDF
AD LDS parent dist name.
MS-RepValMetadataExt.LDF
AD LDS RepValueMetaDataExt.
MS-SecretAttributeCARs.LDF
AD LDS Secret Attribute Control Access Rights
< Back
Next >
Cancel
Help

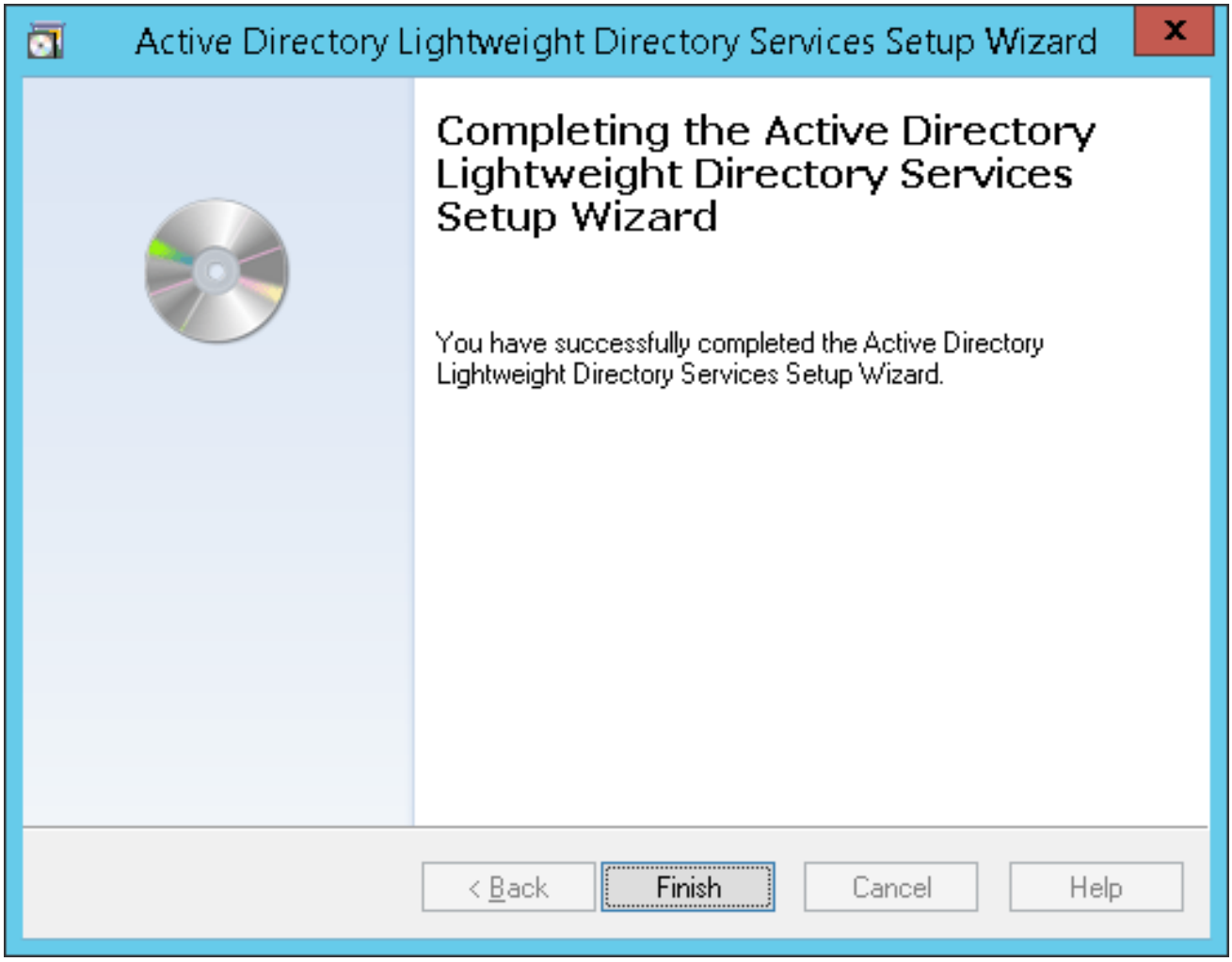


10. Click **Next** in order to start the installation.


Active Directory Lightweight Directory Services Setup Wizard
Ready to Install
The AD LDS Setup Wizard is ready to install AD LDS with the following configuration.
Before continuing, review and confirm your selections.
Selections:
Install a unique instance of AD LDS.
Instance name: MultiForest
Computers will connect to this instance of AD LDS using the following ports:
LDAP port: 50000
SSL port: 50001
AD LDS replication will use Negotiate authentication.
Store AD LDS data files in the following location:
To change your selections, click Back. To install AD LDS, click Next.
< Back
Next >
Cancel
Help



11. The installation is completed successfully. Click **Finish**.



Configure ADAM Schema Analyzer

If the user IDs (sAMAccountNames) are unique across different domains and there are not multiple users with the same ID in different domains of different forests, then the users can be synchronized from the AD to the respective forests on the AD LDS, all of which can exist on a single partition on the AD LDS in a **multi forest** setup. For example, consider the figure in the Active Directory Multiple Forest Support Scenario in CUCM section, and if a user ID 'alice' exists in only one of the three domains the setup in this scenario would be as follows:

PARTITION	FOREST	DN
P1	cisco.com	DC=cisco,DC=com
	webex.com	DC=webex, DC=cisco,DC=com
	tandberg.com	DC=Tandberg, DC=cisco,DC=com

In order to configure CUCM with AD LDS, the user ID (sAMAccountName) needs to be unique across all the forests. CUCM currently supports only a single partition in AD LDS.

If the sAMAccountNames are not unique, consider using any of these attributes if they uniquely identify a user account - email, telephoneNumber, employeeNumber, uid, or userPrincipalName - and follow the single partition setup.

Note: The multi partition setup explained is for information only and not supported by CUCM.

If there are multiple users with the same user ID (sAMAccountName) in the different domains of the different forests, you need to create one application directory partition in AD LDS for each domain you want to synchronize. So, all the forests will be configured on the AD LDS in a multi partition setup. For example, consider the setup in Active Directory Multiple Forest Support Scenario in CUCM section, and there is a user ID 'alice' in all three domains (webex.com, Tandberg.com, and cisco.com). They will be configured on the AD LDS in a multi partition setup.

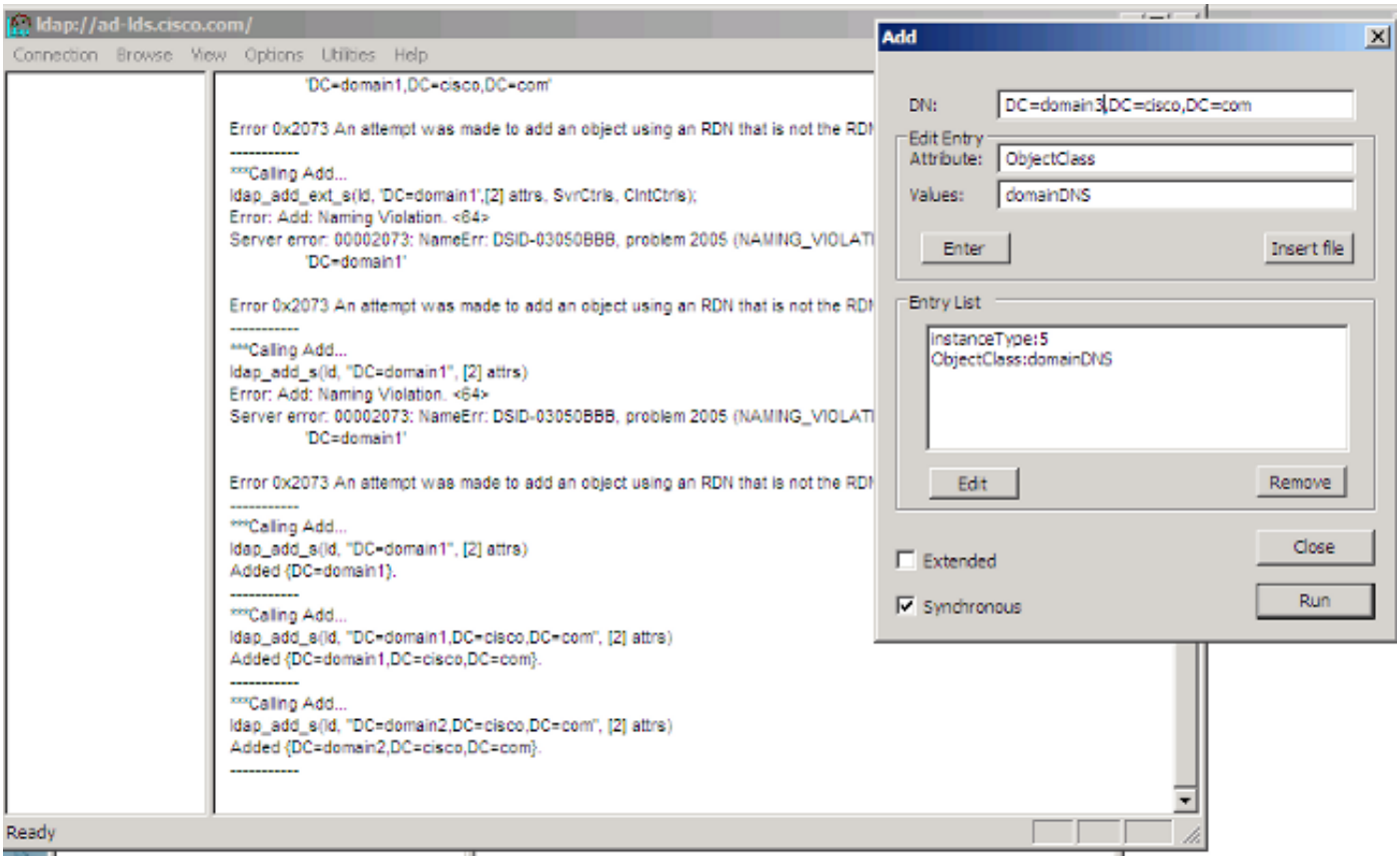
See the Microsoft document on how to create an Application Directory Partition, Step 5: Practice Working with Application Directory Partitions for more information.

In this example, there is a top domain cisco.com, and there will be three directory partitions (webex.com, Tandberg.com, and cisco.com) created under it, one for each domain that you want to synchronize with AD LDS.

PARTITION	FOREST	DN
P1	cisco.com	DC=cisco,DC=com
P2	webex.com	DC=webex, DC=cisco,DC=com
P3	tandberg.com	DC=Tandberg, DC=cisco,DC=com

where each forest is configured in a separate application directory partition on the AD LDS.

Note: The ObjectClass needs to be domainDNS and not container as referenced in the Microsoft document.



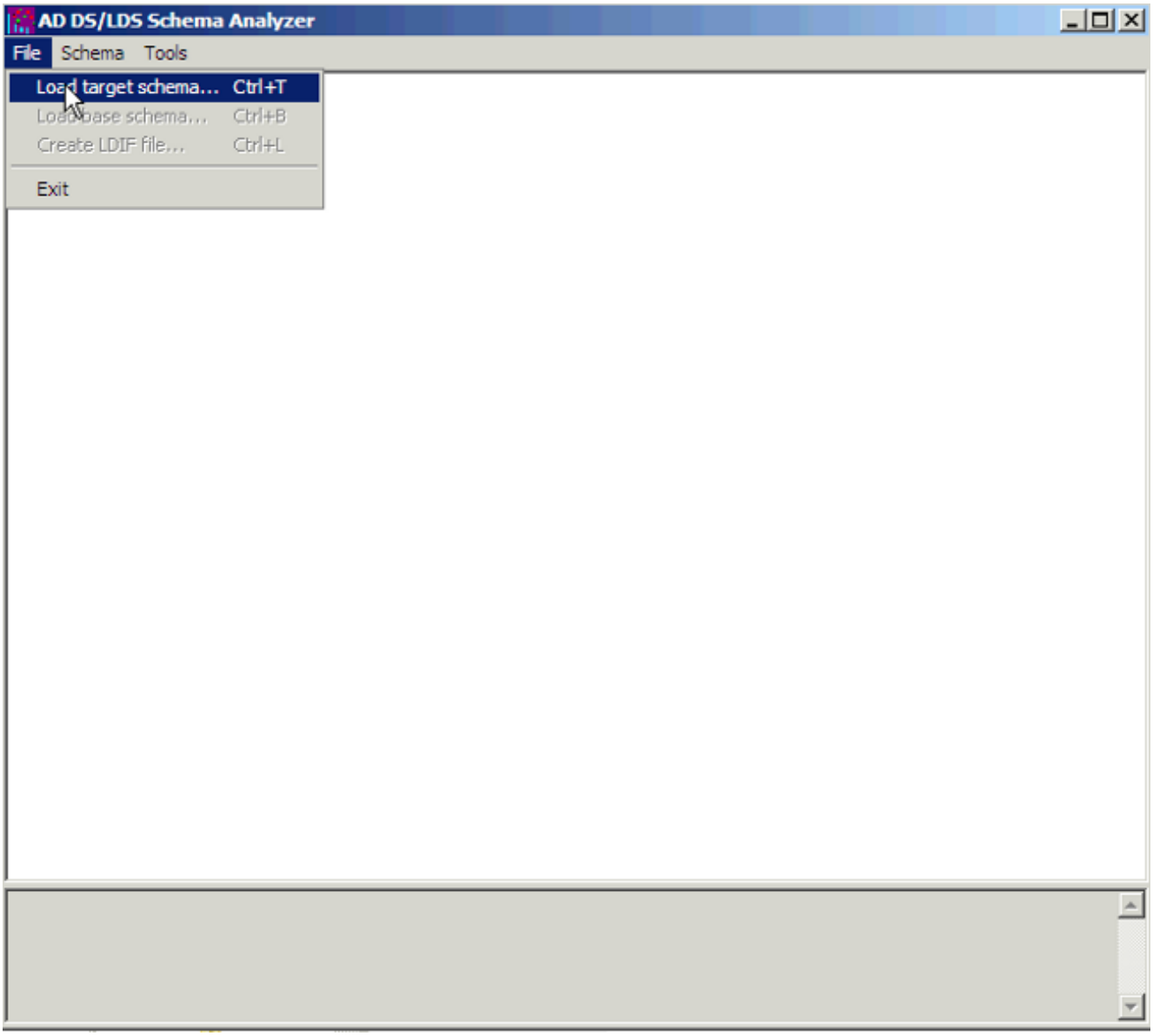
This process to create a directory partition for each domain that you want to synchronize against works based on LDAP referral (RFC 2251) and requires that the LDAP client (CUCM, CUP, and so on) supports referrals.

Copy the schema from each domain to ADAM. This process needs to be repeated for each domain (in this example you would need to repeat this three times, one per each Domain Controller that you have) that you need to synchronize to.

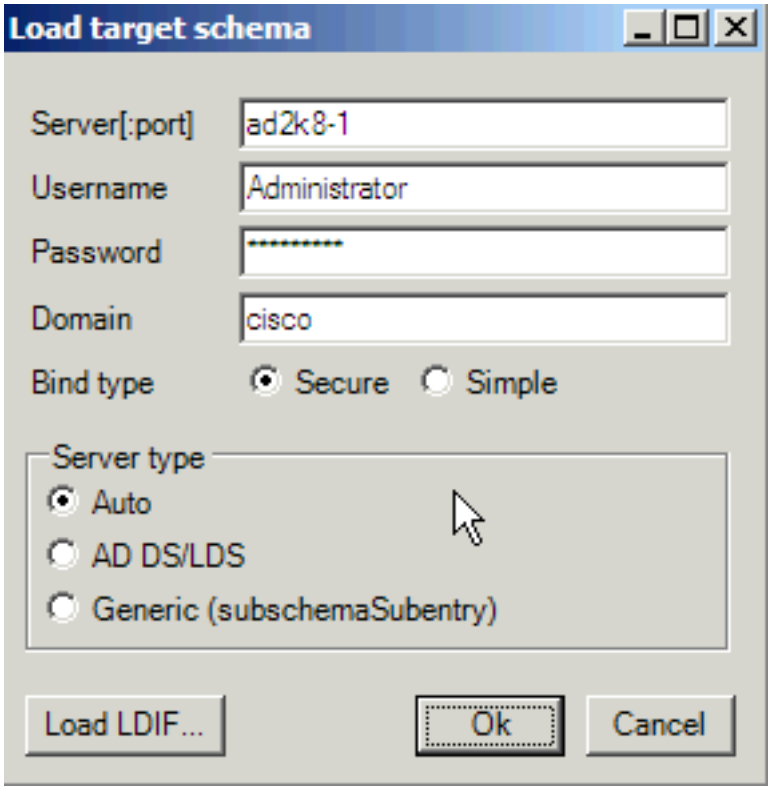
Directory synchronization with a multi partition setup in AD LDS will work, however, Directory Authentication in that setup is not supported by CUCM.

Note: This example shows the process against one a single partition.

1. Copy the schema from the domain to ADAM.
2. Open AD DS/LDS schema analyzer (ADSchemaAnalyzer.exe) in the directory c:\windows\adam.
3. Choose **File > Load target schema**.

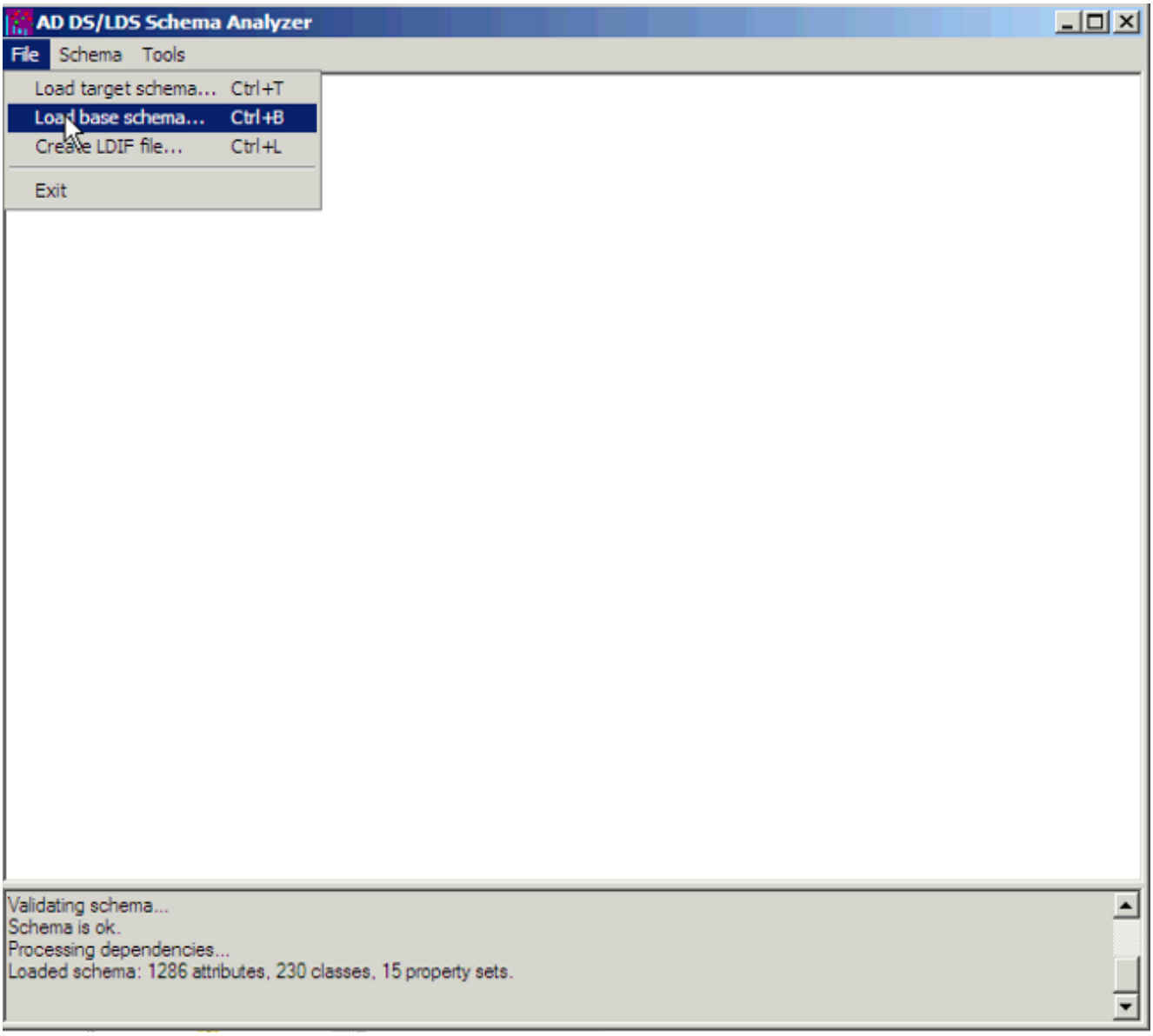


4. Provide the credentials of the source AD Domain Controller that you want to import from.

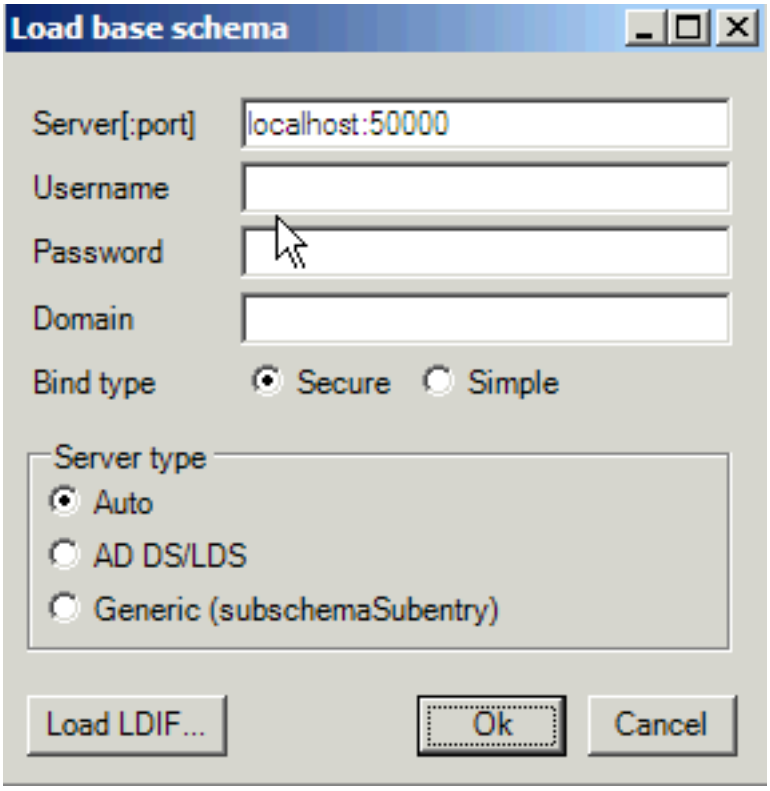


Click **Ok**.

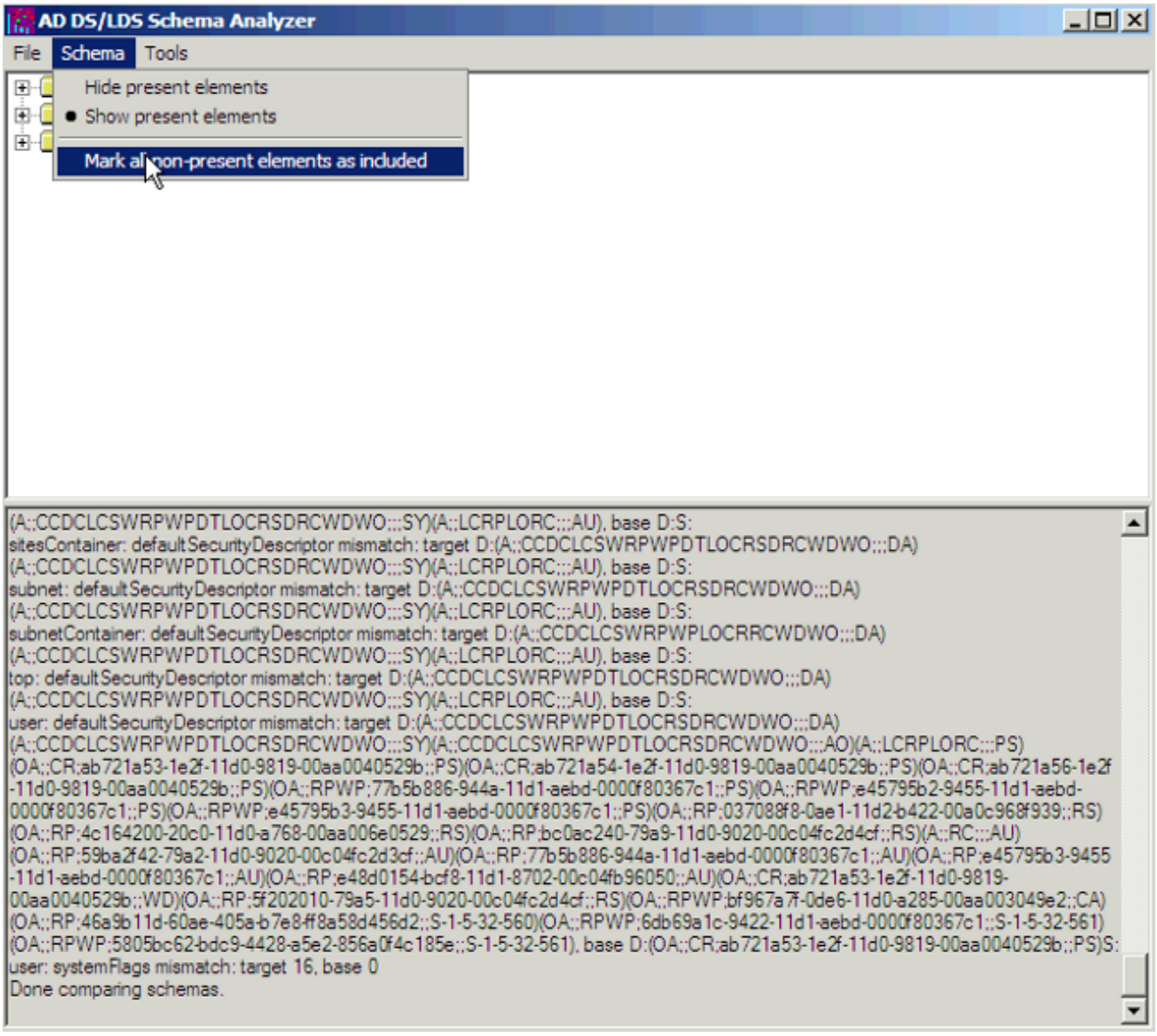
5. Choose **File > Load base schema**.



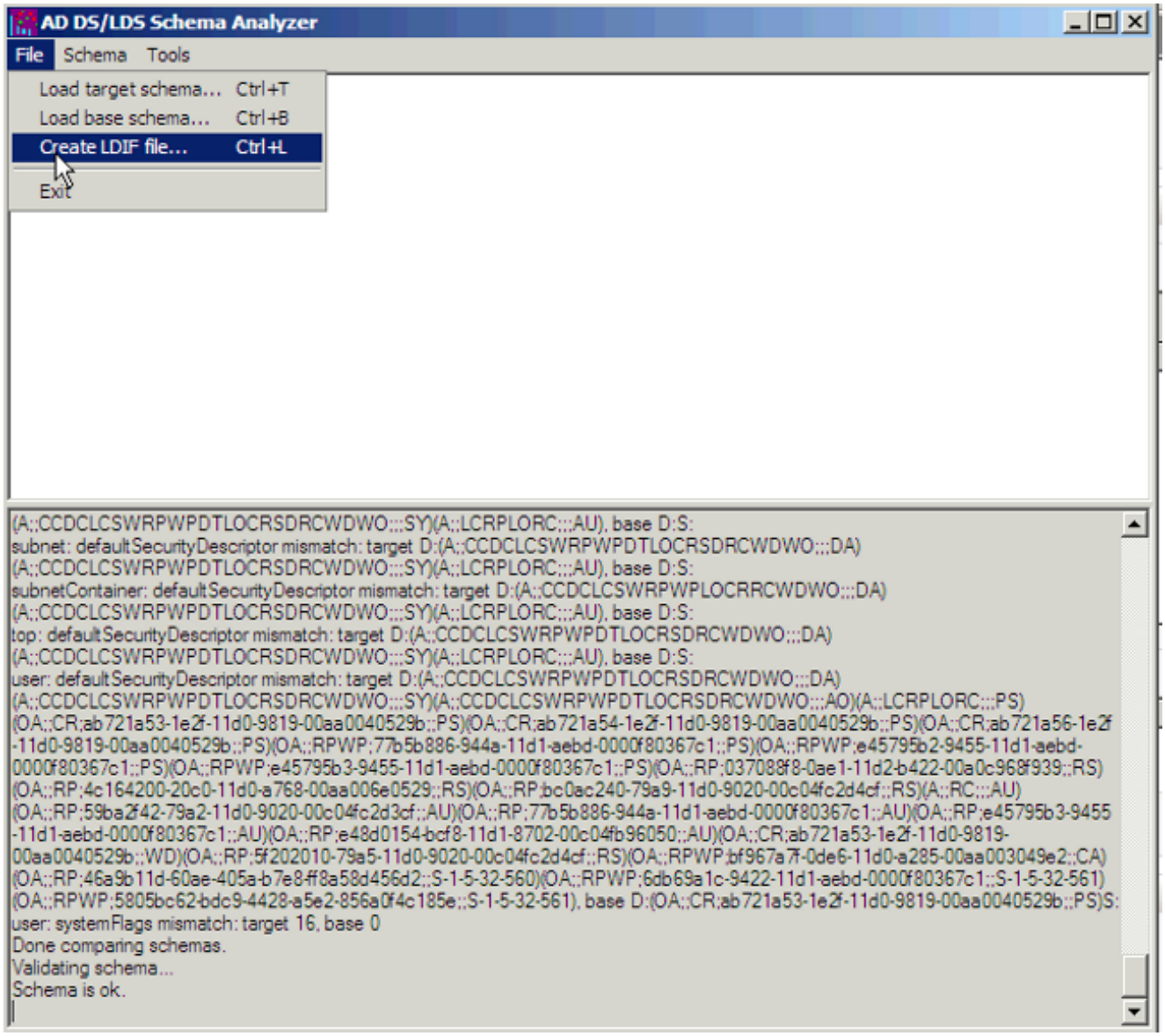
6. Specify the AD LDS to which you want to connect and extend the schema. Click **Ok**.



7. Choose **Schema > Mark all non-present elements as included**.



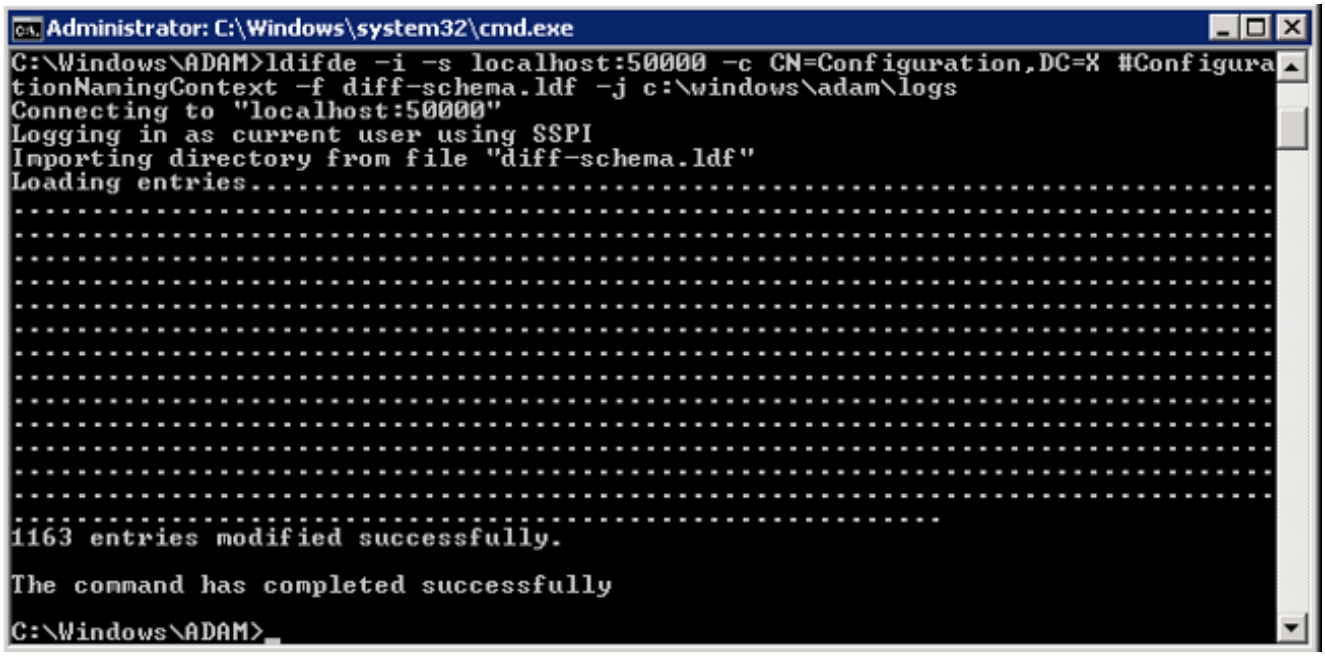
8. Choose **File > Create LDIF file**. In this example, the file created via this step is diff-schema.ldf. In order to simplify the process the file should be created in c:\windows\adam.



An option available to help organize the files that need to be generated is to create a separate directory in order to allow for these files to be separated from the main c:\windows\adam directory. Open a command prompt and create a log directory in c:\windows\adam. `cd \windows\adam`

`mkdir logs`

9. Import the ldif schema, created with ADSchema Analyzer, to AD LDS. `ldifde -i -s localhost:50000 -c CN=Configuration,DC=X #ConfigurationNamingContext -f diff-schema.ldf -j c:\windows\adam\logs` Refer to Using LDIFDE to import and export directory objects to Active Directory for additional ldifde options and command formats.



Extend the AD LDS Schema with the User-Proxy Objects

The object for the proxy authentication needs to be created and the object class 'user' will not be used. The object class that is created, userProxy, is what allows the bind redirection. The object class detail needs to be created in a ldif file. The file is a creation of a new file, which in this example is MS-UserProxy-Cisco.ldf. This new file is generated from the original MS-UserProxy.ldf and edited, use a text edit program, to have this content:

```
#------------------------------------------------------------------
# @@UI-Description: AD LDS simple userProxy class.
#
# This file contains user extensions for default ADAM schema.
# It should be imported with the following command:
# ldifde -i -f MS-UserProxy.ldf -s server:port -b username domain password -k -j . -c
"CN=Schema,CN=Configuration,DC=X" #schemaNamingContext
#
#------------------------------------------------------------------

dn: CN=User-Proxy,CN=Schema,CN=Configuration,DC=X
changetype: ntdsSchemaAdd
objectClass: top
objectClass: classSchema
cn: User-Proxy
subClassOf: top
governsID: 1.2.840.113556.1.5.246
schemaIDGUID:: bxjWYLbzmEiwrWU1r8B2IA==
rDNAttID: cn
showInAdvancedViewOnly: TRUE
adminDisplayName: User-Proxy
adminDescription: Sample class for bind proxy implementation.
objectClassCategory: 1
lDAPDisplayName: userProxy
```

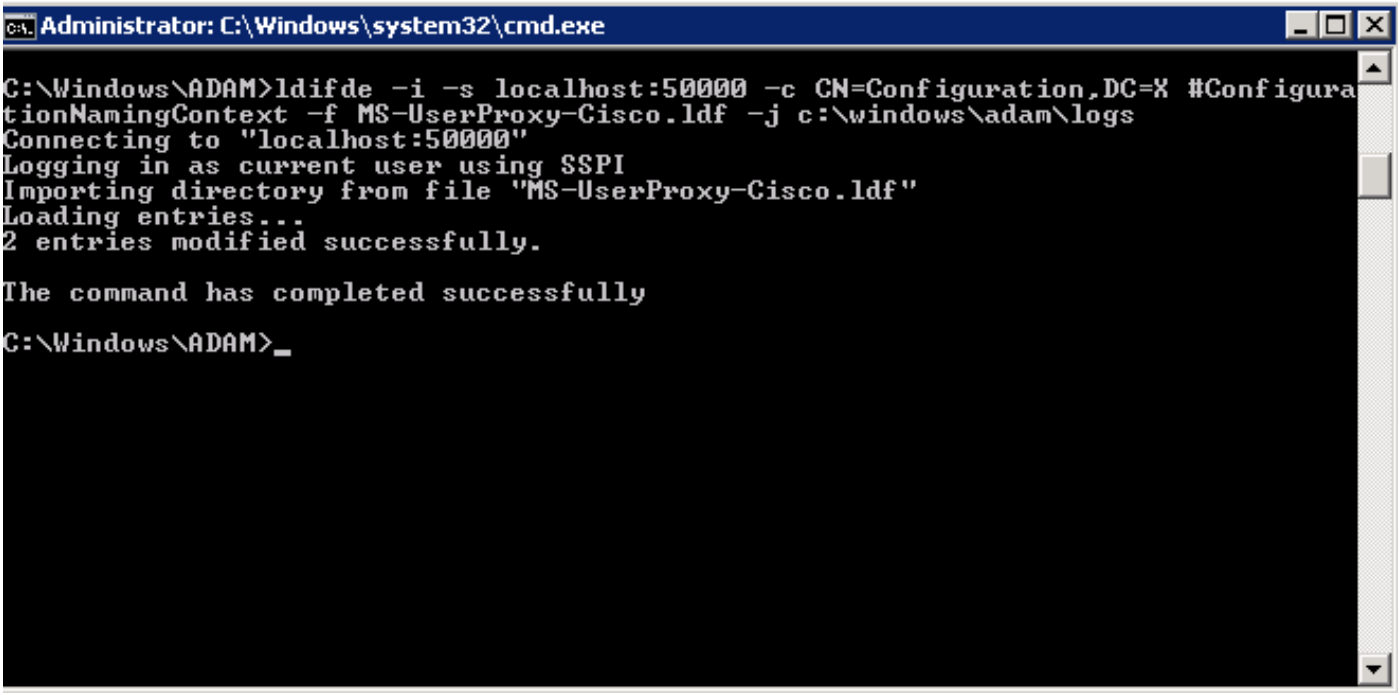
```
systemOnly: FALSE
possSuperiors: domainDNS
possSuperiors: organizationalUnit
possSuperiors: container
possSuperiors: organization
defaultSecurityDescriptor:
D:(OA;;CR;ab721a53-1e2f-11d0-9819-00aa0040529b;;PS)S:
defaultHidingValue: TRUE
defaultObjectCategory: CN=User-Proxy,CN=Schema,CN=Configuration,DC=X
systemAuxiliaryClass: msDS-BindProxy
systemMayContain: userPrincipalName
systemMayContain: givenName
systemMayContain: middleName
systemMayContain: sn
systemMayContain: manager
systemMayContain: department
systemMayContain: telephoneNumber
systemMayContain: mail
systemMayContain: title
systemMayContain: homephone
systemMayContain: mobile
systemMayContain: pager
systemMayContain: msDS-UserAccountDisabled
systemMayContain: samAccountName
systemMayContain: employeeNumber
systemMayContain: initials
systemMayContain: ipPhone
systemMayContain: displayName
systemMayContain: msRTCSIP-primaryuseraddress
systemMayContain: uid

dn:
changetype: modify
add: schemaUpdateNow
schemaUpdateNow: 1
-
```

Save MS-UserProxy-Cisco.ldf file in C:\windows\adam.

Import the new object class to AD LDS.

```
ldifde -i -s localhost:50000 -c CN=Configuration,DC=X #ConfigurationNamingContext -f
MS-UserProxy-Cisco.ldf -j c:\windows\adam\logs
```



Import the Users From AD DC to AD LDS

The user from each domain now needs to be imported to AD LDS. This step needs to be repeated for each domain that needs to synchronize. This example only shows the process against one of the domains. Start with the original MS-AdamSyncConf.xml and create an XML file for each domain that needs to be synchronized and modify the file with the details specific to each domain to have this content:

```
<?xml version="1.0"?>
<doc>
 <configuration>
 <description>Adam-Sync1</description>
 <security-mode>object</security-mode>
 <source-ad-name>ad2k8-1</source-ad-name>
 <source-ad-partition>dc=cisco,dc=com</source-ad-partition>
 <source-ad-account></source-ad-account>
 <account-domain></account-domain>
 <target-dn>dc=cisco,dc=com</target-dn>
 <query>
  <base-dn>dc=cisco,dc=com</base-dn>
   <object-filter>
(&#124;(&amp;(!cn=Administrator)(!cn=Guest) (!cn=ASPNET)
(!cn=krbtgt)(sAMAccountType=805306368))(&amp;(objectClass=user)(isDeleted=TRUE)))
    </object-filter>
  <attributes>
   <include>objectSID</include>
   <include>mail</include>
   <include>userPrincipalName</include>
   <include>middleName</include>
   <include>manager</include>
```

```
   <include>givenName</include>
   <include>sn</include>
   <include>department</include>
   <include>telephoneNumber</include>
   <include>title</include>
   <include>homephone</include>
   <include>mobile</include>
   <include>pager</include>
   <include>msDS-UserAccountDisabled</include>
   <include>samAccountName</include>
   <include>employeeNumber</include>
<include>initials</include>
<include>ipPhone</include>
<include> displayName</include>
<include> msRTCSIP-primaryuseraddress</include>
<include>uid</include>
   <exclude></exclude>
  </attributes>
 </query>
 <user-proxy>
   <source-object-class>user</source-object-class>
   <target-object-class>userProxy</target-object-class>
 </user-proxy>
 <schedule>
  <aging>
   <frequency>0</frequency>
   <num-objects>0</num-objects>
  </aging>
  <schtasks-cmd></schtasks-cmd>
 </schedule>
 </configuration>
 <synchronizer-state>
 <dirsync-cookie></dirsync-cookie>
 <status></status>
 <authoritative-adam-instance></authoritative-adam-instance>
 <configuration-file-guid></configuration-file-guid>
 <last-sync-attempt-time></last-sync-attempt-time>
 <last-sync-success-time></last-sync-success-time>
 <last-sync-error-time></last-sync-error-time>
 <last-sync-error-string></last-sync-error-string>
 <consecutive-sync-failures></consecutive-sync-failures>
 <user-credentials></user-credentials>
 <runs-since-last-object-update></runs-since-last-object-update>
 <runs-since-last-full-sync></runs-since-last-full-sync>
 </synchronizer-state>
</doc>
```

In this file, these tags should be replaced to match the domain:

- <*source-ad-name*> - Use the host name of the domain.
- <*source-ad-partition*> - Use the root partition from the source AD DC that you want to import from (for example, dc=Cisco, dc=com, or dc=Tandberg, dc=com).
- <base-dn> - Choose the container from which to import from. For example, if all users of the domain are required this should be the same as <source-ad-partition>, but if users are from a specific organizational unit (such as Finance OU), it should be similar to OU=Finance, DC=Cisco, DC=com.

Refer to Search Filter Syntax for more information on how to create an <object-filter>.

Save the newly created XML file in C:\windows\adam.

Open a command window, *cd \windows\adam*.

Enter the command, **ADAMSync /install localhost:50000 c:\windows\ADAM\AdamSyncConf1.xml /log c:\windows\adam\logs\install.log**.

Verify that the file AdamSyncConf1.xml is the newly created XML file.

Synchronize the users with the command **ADAMSync /sync localhost:50000 "dc=cisco,dc=com" /log c:\windows\adam\logs\sync.log**.

The result should be similar to:

In order to complete an automatic sync from AD to ADAM , use the Task scheduler in Windows.

Create a .bat file with this content in it:

"C:\Windows\ADAM\ADAMSync" /install localhost:50000 c:\windows\ADAM\AdamSyncConf1.xml /log c:\windows\adam\logs\install.log

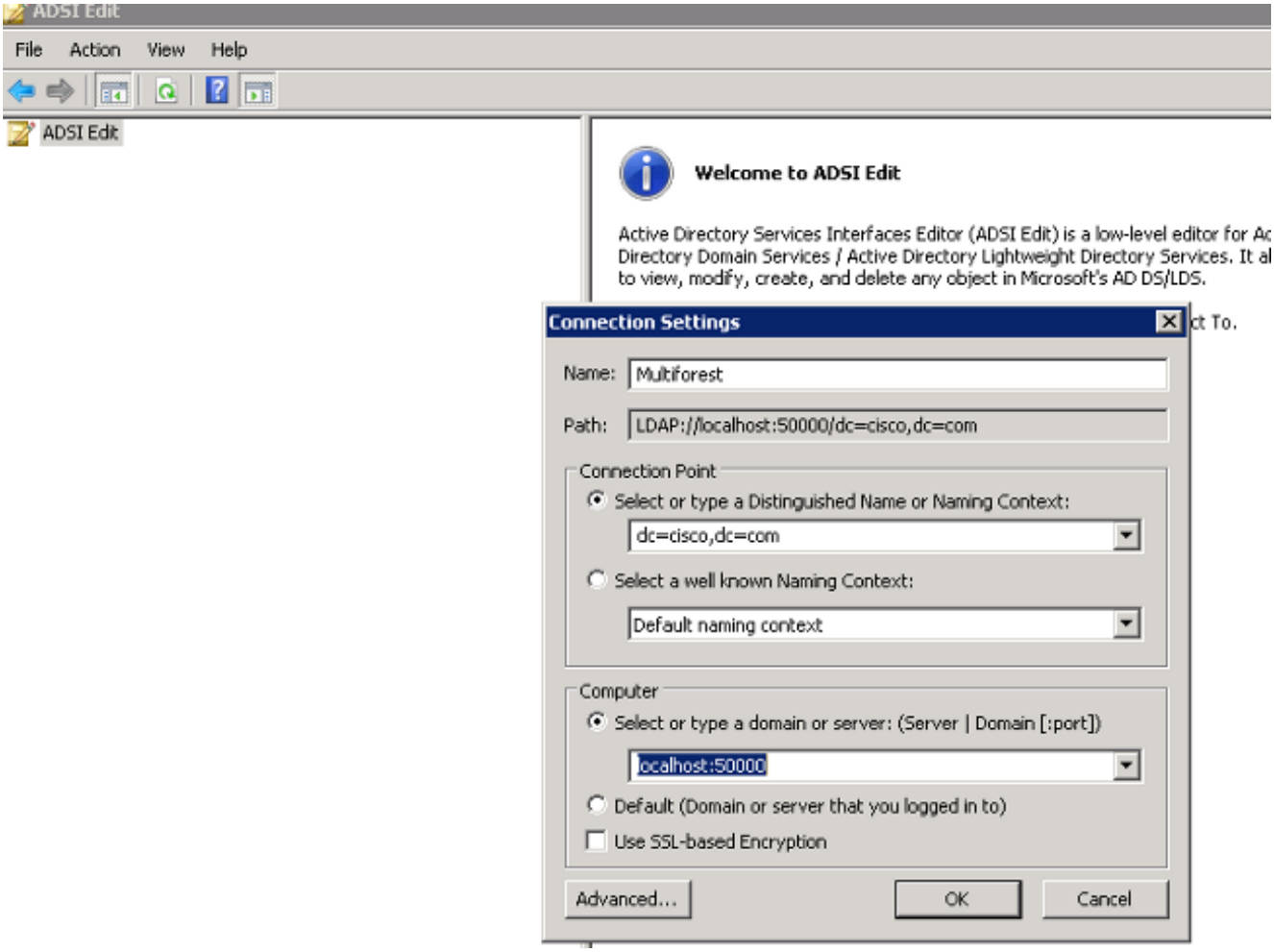
"C:\Windows\ADAM\ADAMSync" /sync localhost:50000 "dc=cisco,dc=com" /log c:\windows\adam\logs\syn.log

Schedule the task to run the .bat file as and when required. This takes care of additions, modifications, and deletions that happen in AD to be reflected in ADAM as well.

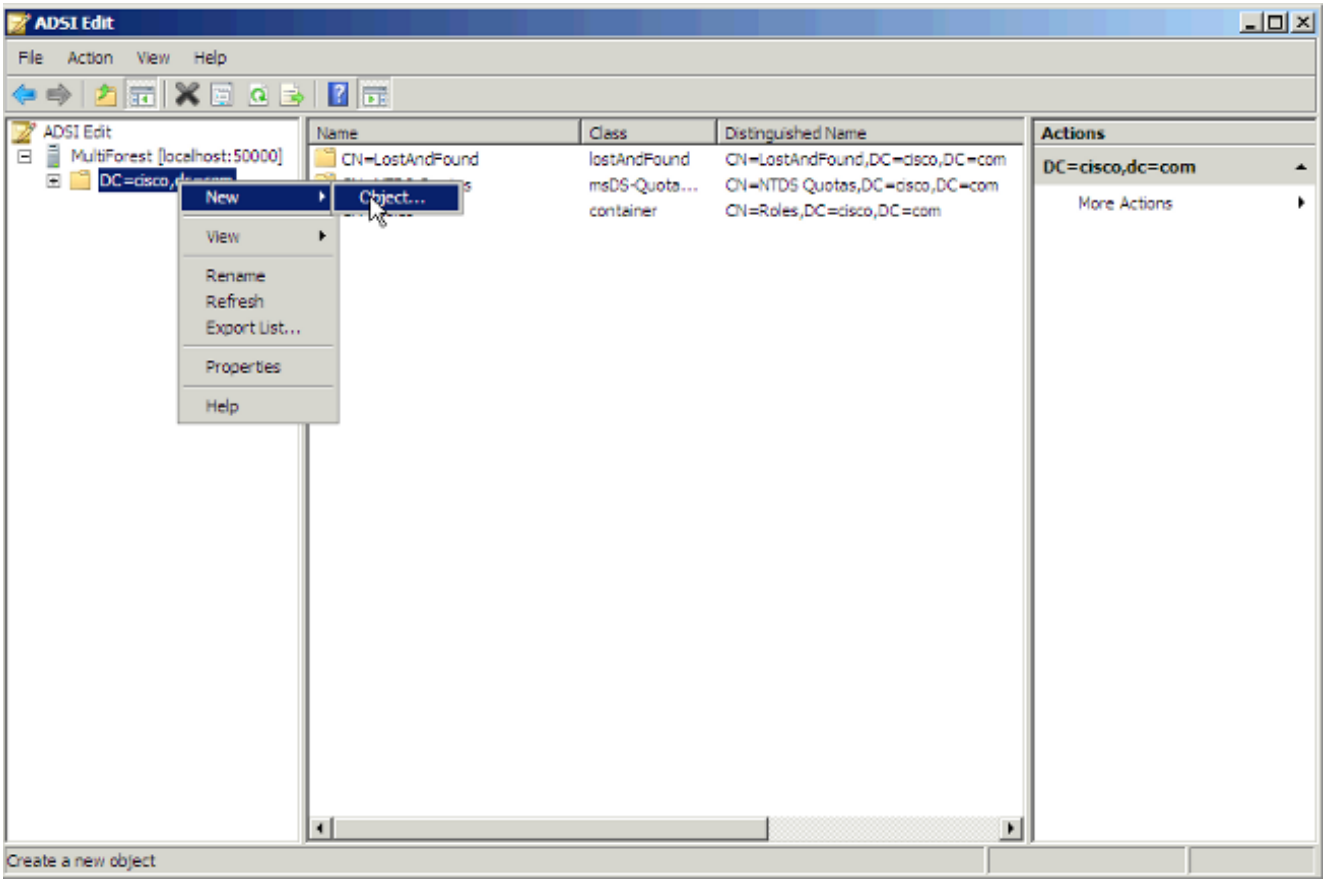
You can create another .bat file and schedule it to complete an automatic sync from the other forest.

Create the User in AD LDS for CUCM Synchronization and Authentication

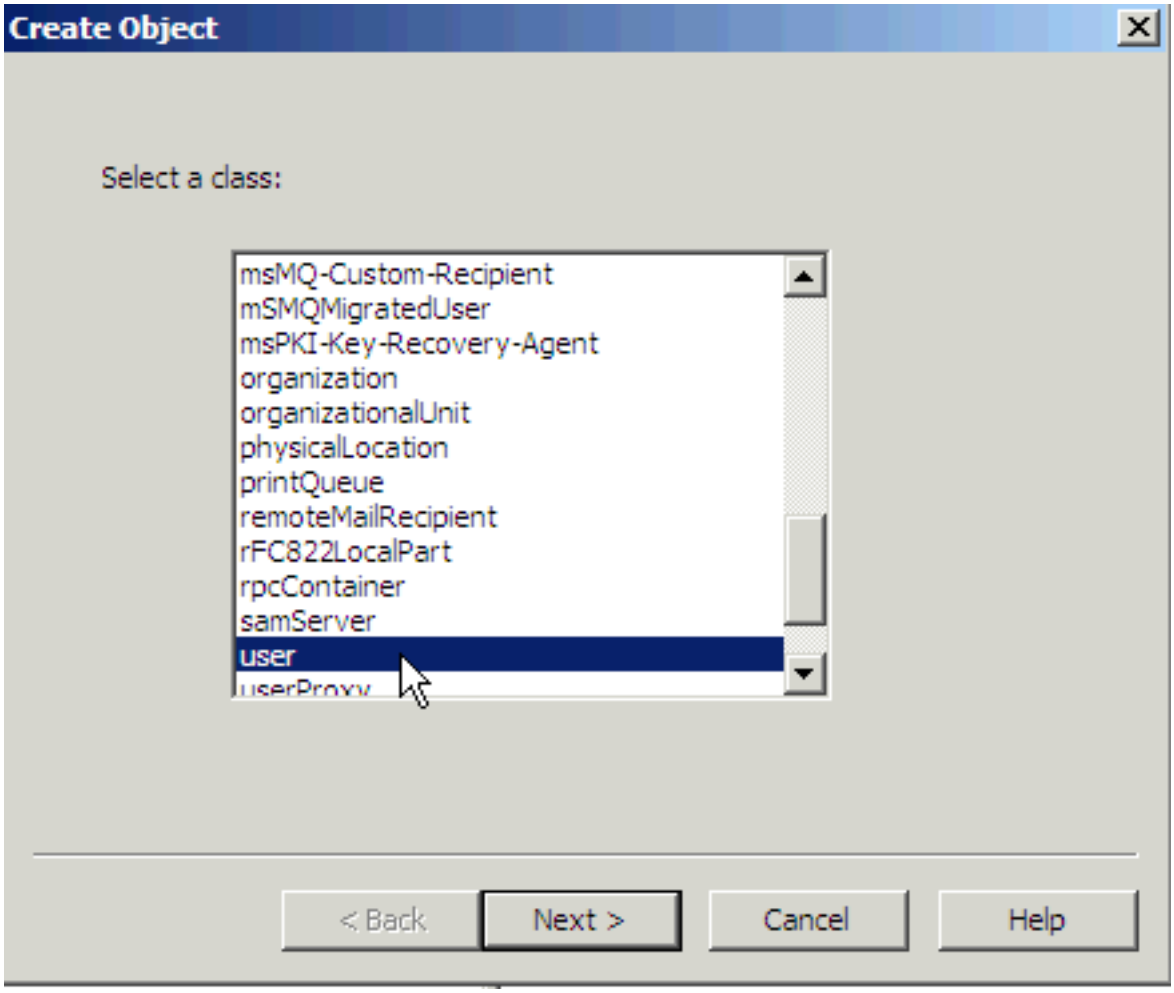
1. Open ADSI Edit from the Administrator tools in the Startup menu.
2. Choose **File > Connection** (or **Action > Connect To**).
3. Connect to base dn of the AD LDS tree (DC=Cisco,DC=com) and specify the host and port where it is hosted (localhost:50000). Click **OK**.



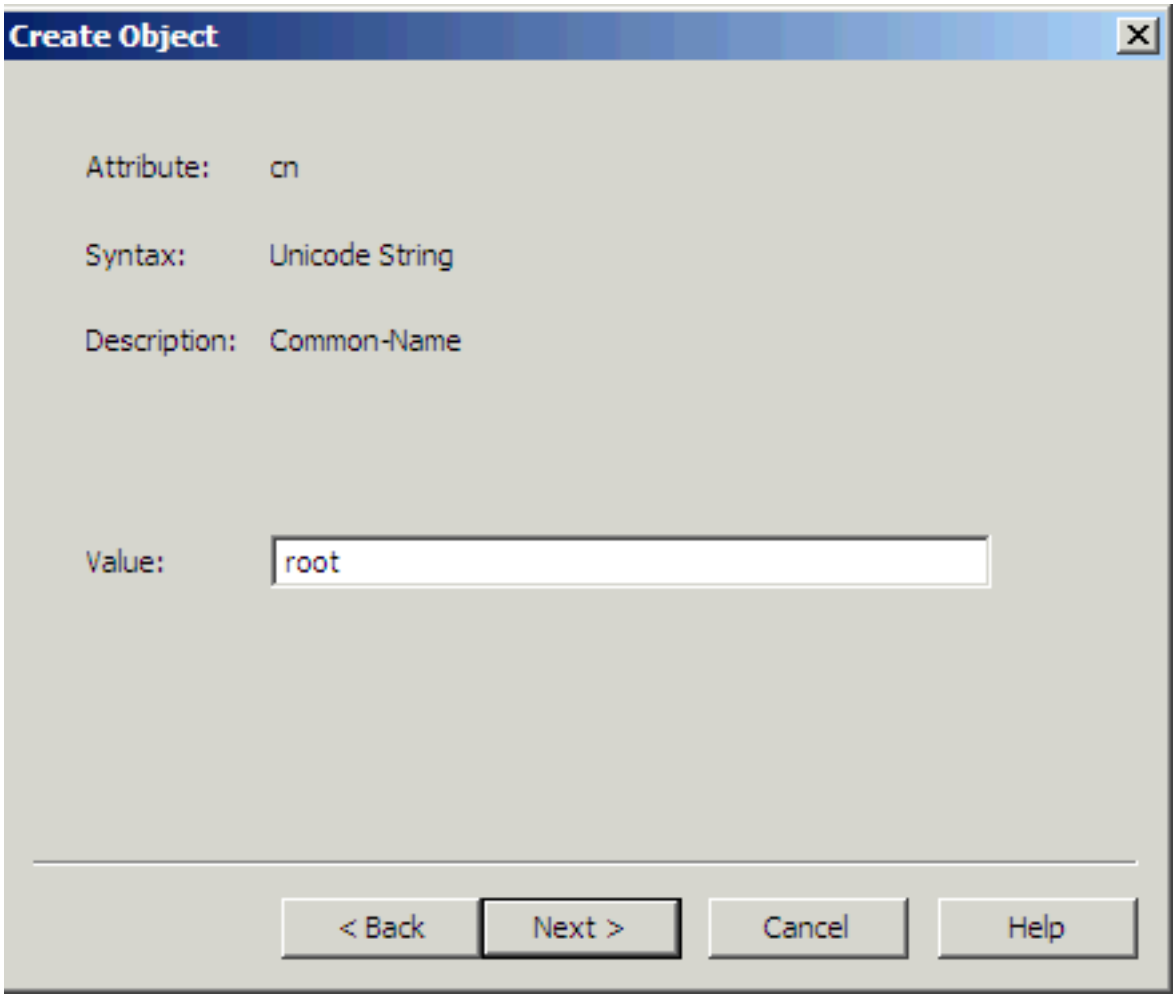
4. Right-click the base DN and choose **New > Object**.



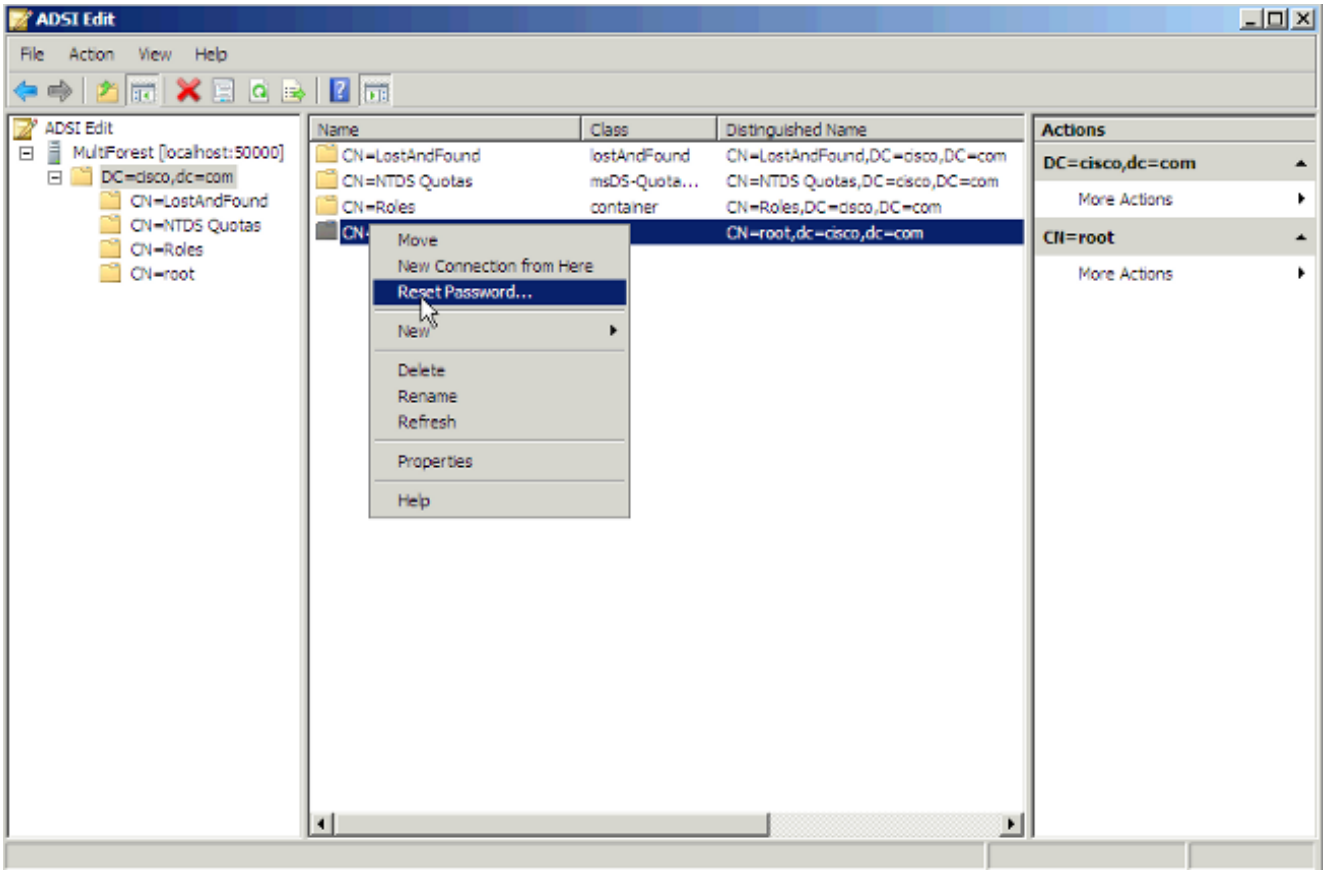
5. Choose **user**. Click **Next**.



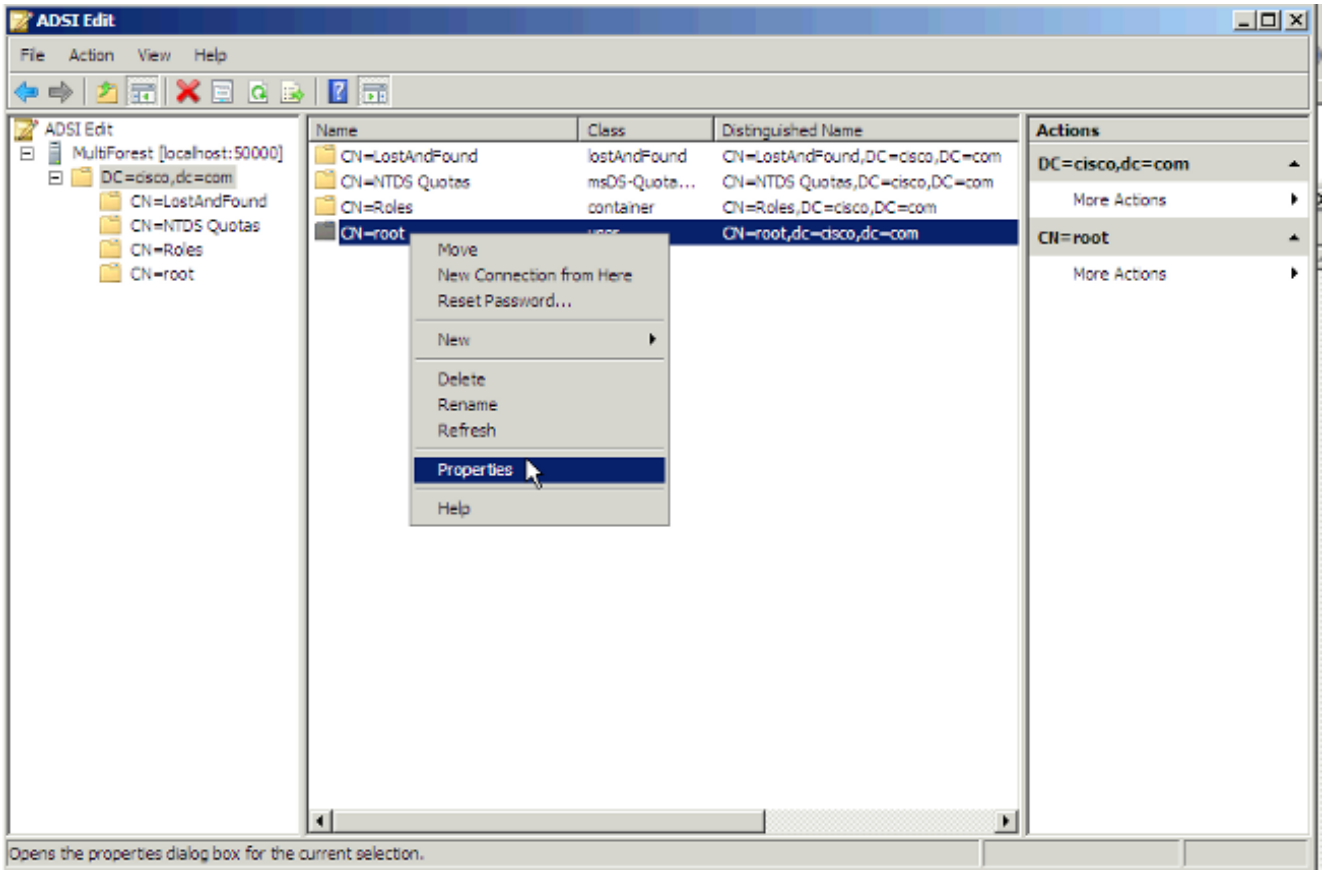
6. In the Value field, enter the chosen object name. In this example "root" is the chosen name (any name could be chosen here). Click **Next**.



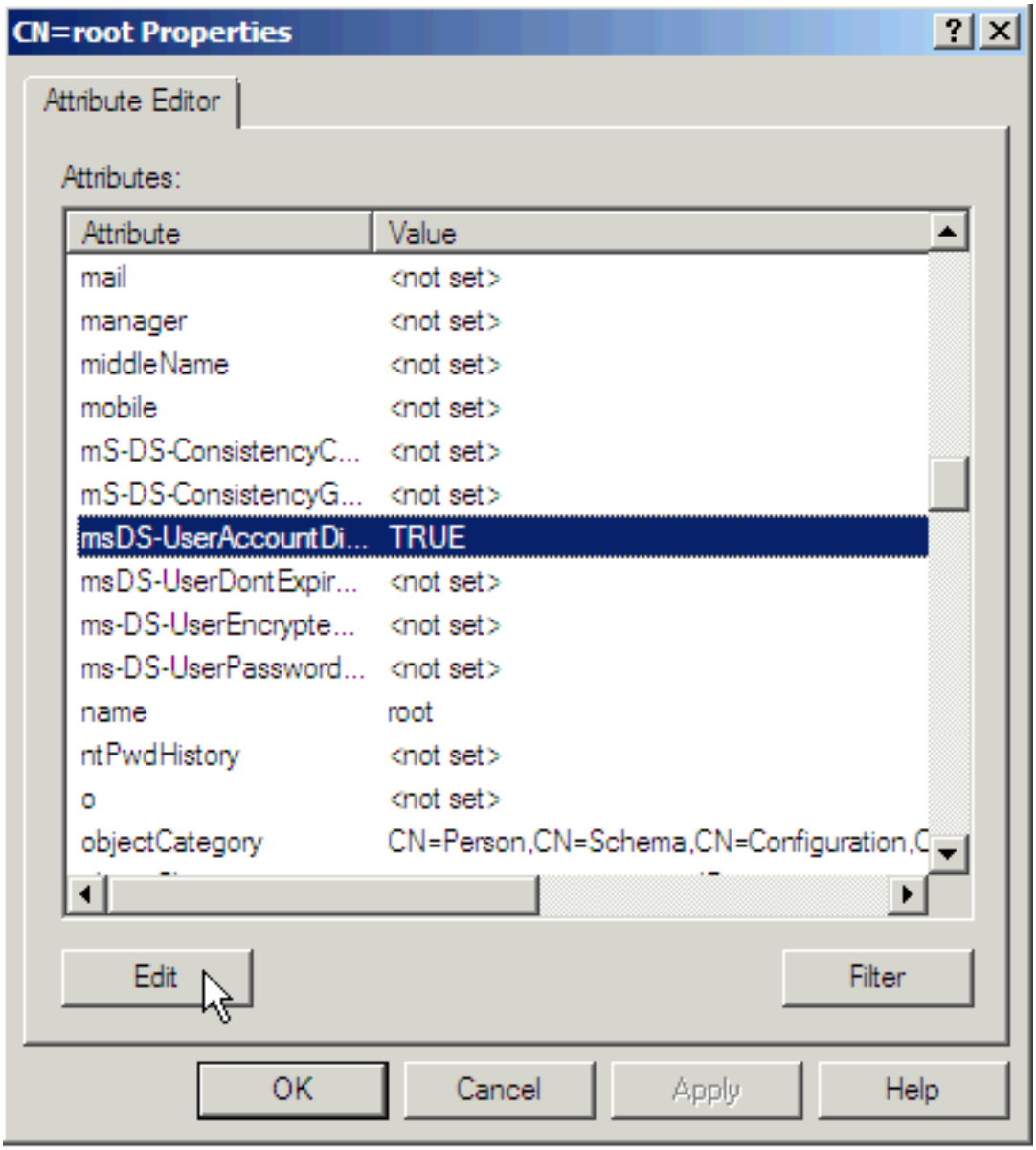
7. In order to provide a password to the new user, right-click the user and choose **Reset Password**.



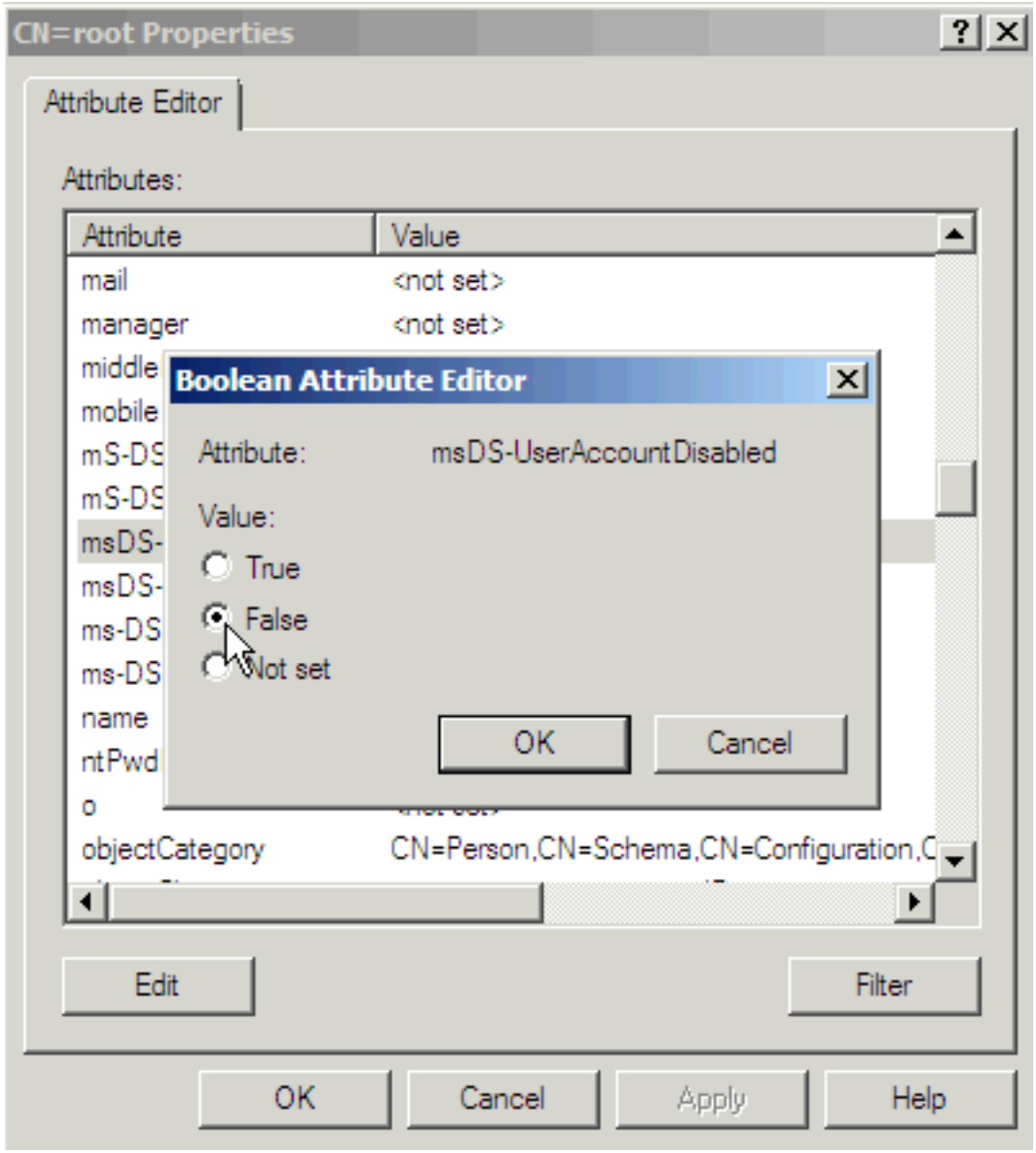
8. The new user is disabled by default. In order to enable the new user, right-click the user and choose **Properties**.



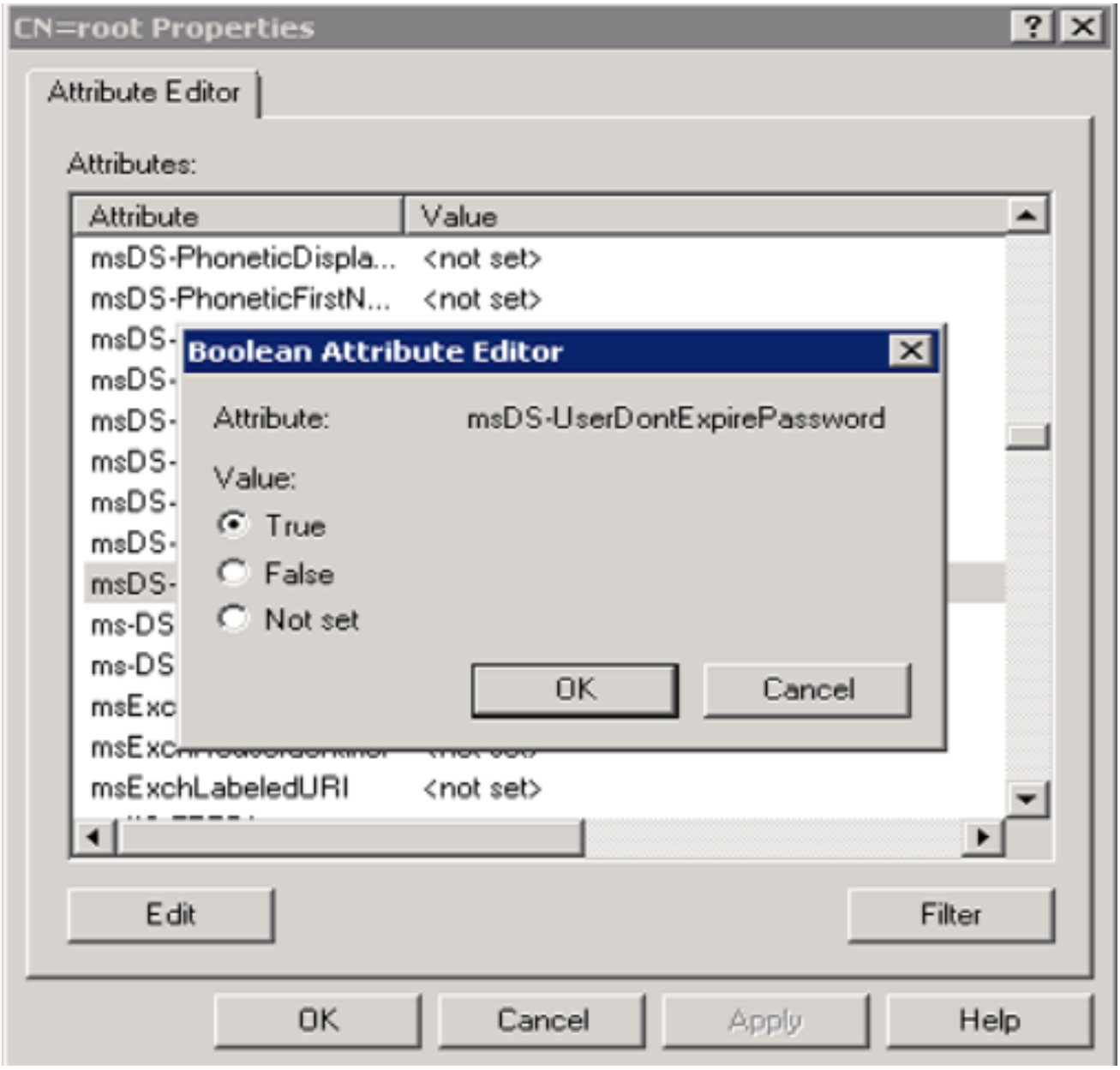
9. Browse to the attribute **msDS-UserAccountDisabled** and click **Edit**.



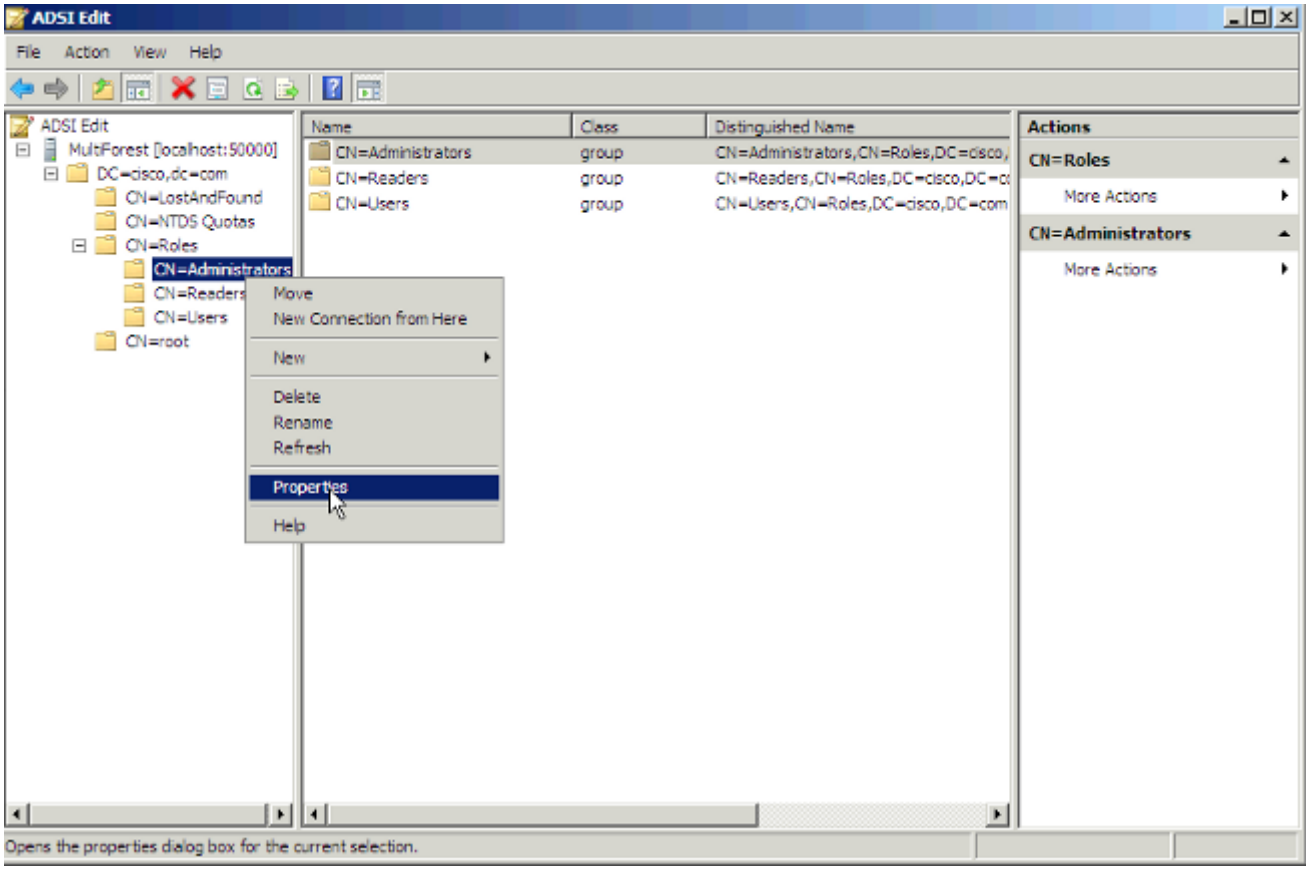
10. Click the **False** radio button in order to enable the user account. Click **OK**.



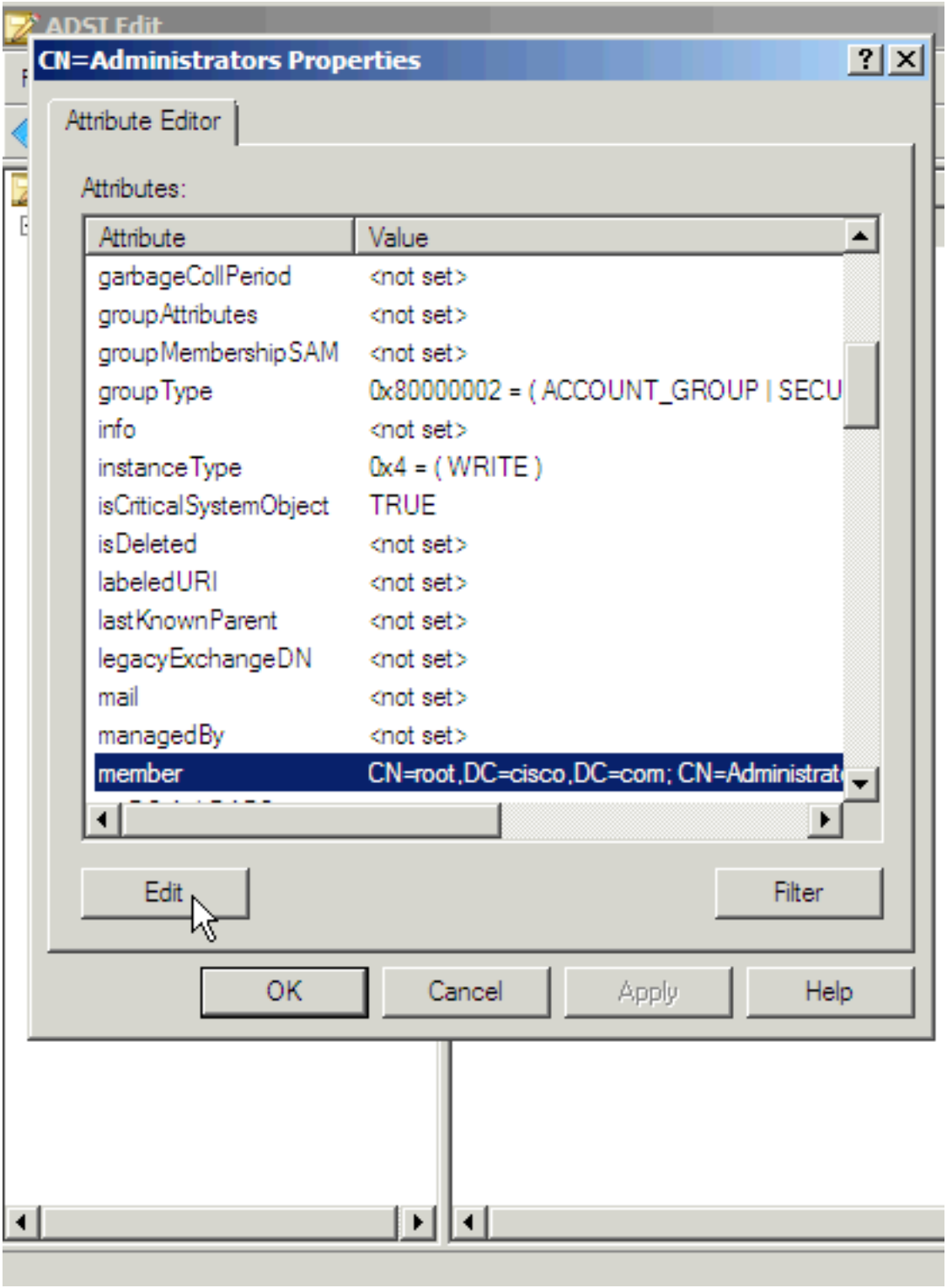
11. Click the **True** radio button in order to ensure the password will never expire. Click **OK**.



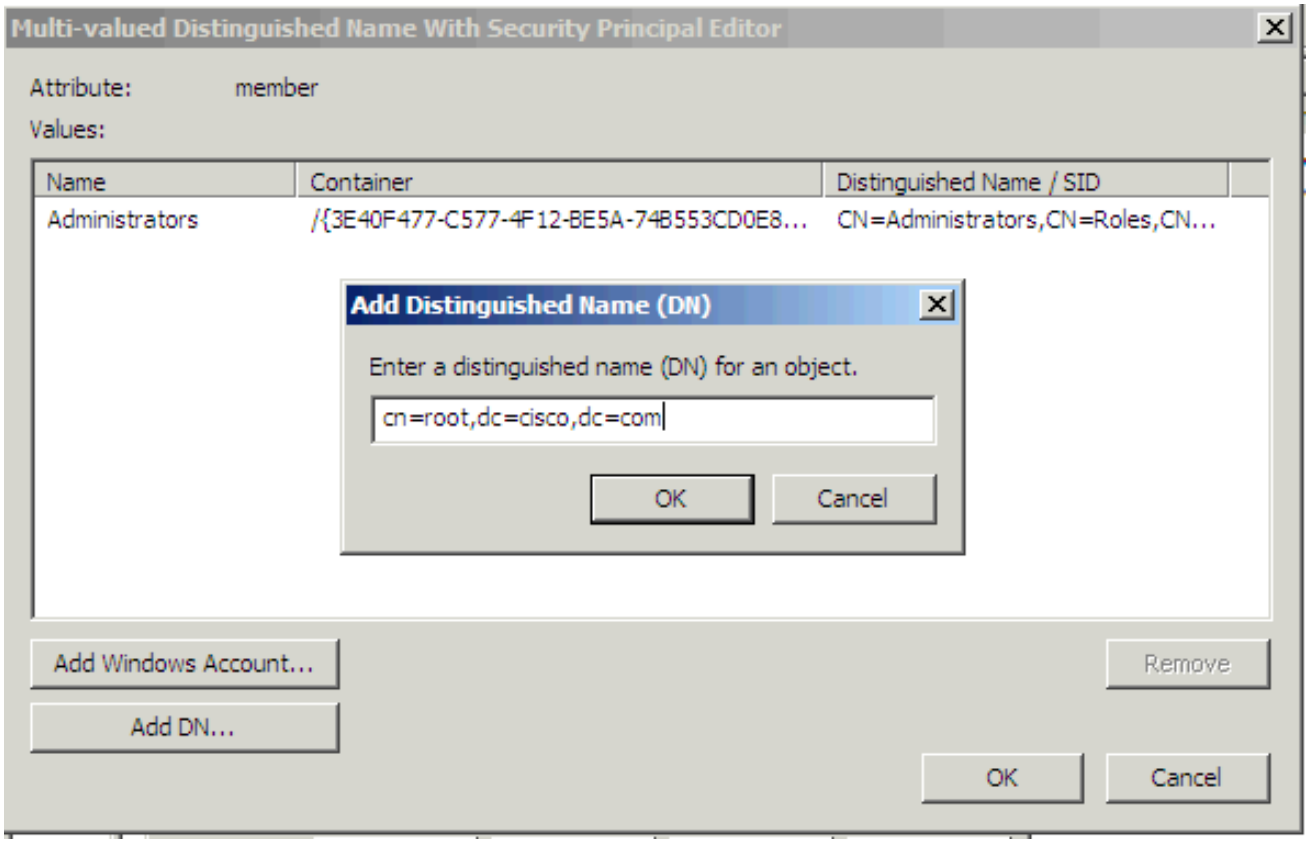
12. The new user needs to be added to one group that has reading permission to the AD LDS, which in this example Administrators was chosen. Browse to **CN=Roles > CN=Administrators**. Right-click CN=Administrators and choose **Properties**.



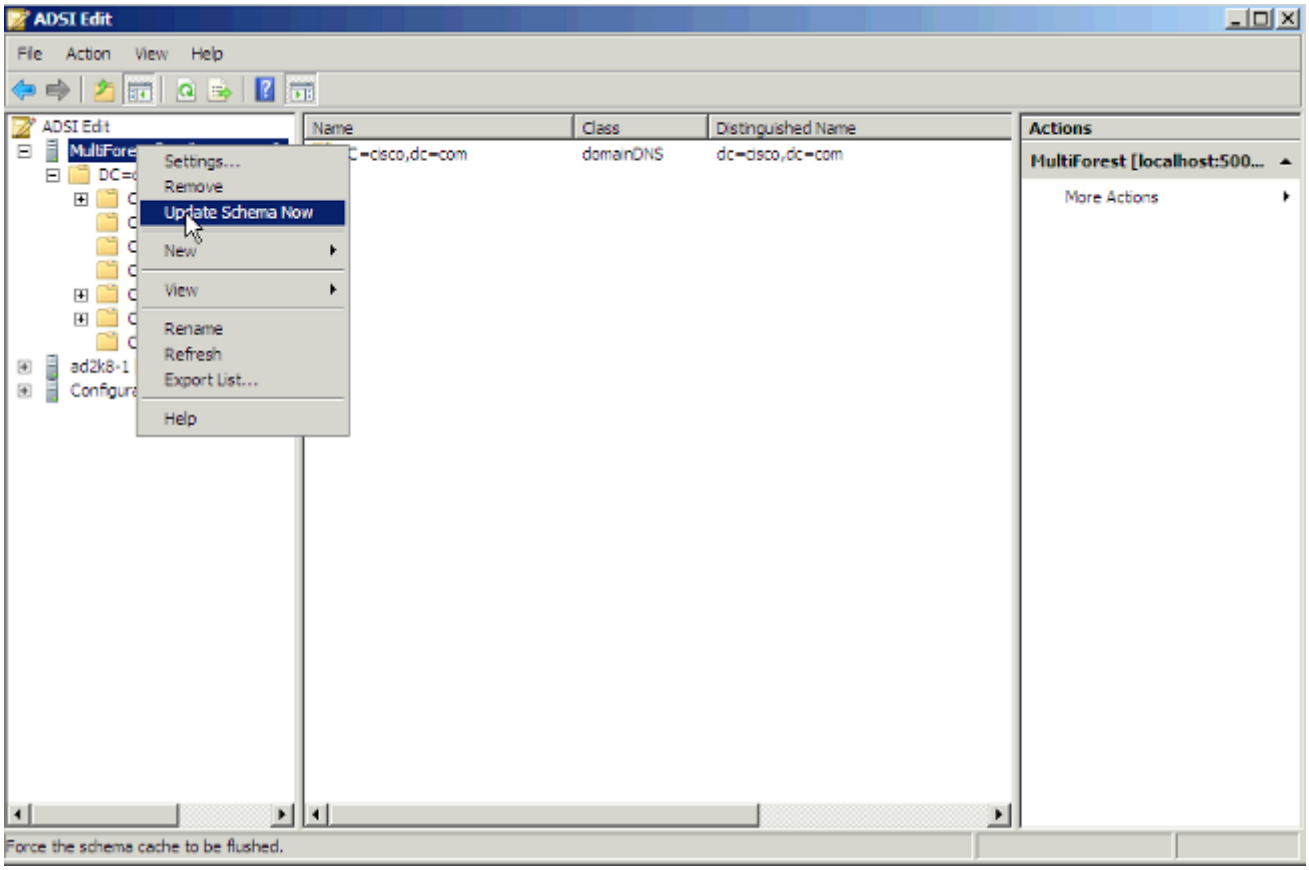
13. Choose the attribute **member** and click **Edit**.

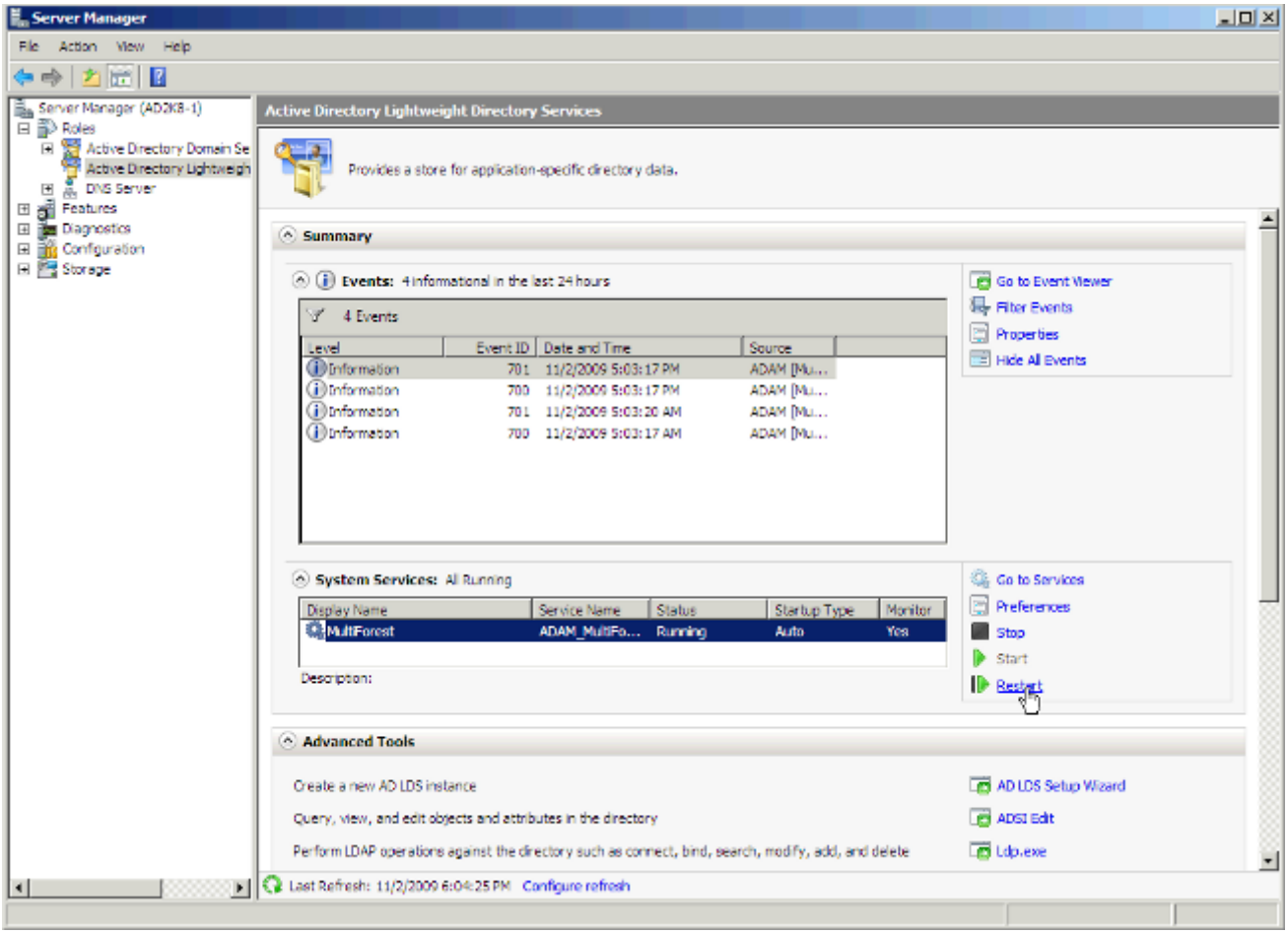


14. Enter the new DN that was created previously, **cn=root,dc=Cisco,dc=com**, to this group. Click **OK**.



15. Choose **Update Schema Now** and restart AD LDS.





Configure Bind Redirection

By default, binding to ADAM with bind redirection requires an SSL connection. SSL requires the installation and use of certificates on the computer that runs ADAM and on the computer that connects to ADAM as a client. If certificates are not installed in your ADAM test environment, you can disable the requirement for SSL as an alternative.

By default, SSL is enabled. In order to make the LDAPS protocol work in ADAM/LDS you will need to generate a certificate.

In this example, the Microsoft Certification Authority Server is used in order to issue the certificate. In order to request a certificate, go to the web page of the Microsoft CA - http://<MSFT CA hostname>/certsrv and complete these steps:

1. Click **Request a certificate**.
2. Click **Advanced certificate request**.

3. Click **Create and submit a request to this CA**.
4. In the Name textbox, enter the full DNS name of the ADAM/AD LDS server.
5. Ensure Type of certificate is **Server authentication certificate**.
6. For the format, choose **PCKS10**.
7. Choose **Mark Keys as exportable**.
8. Optionally, fill in the other information.
9. In the Friendly name textbox, enter the full dns name of the ADAM/AD LDS server.
10. Click **Submit**.

Go back to the certification authority interface and click the **Pending Certificates** folder. Right-click the certificate request made by the ADAM/AD-LDS machine and issue the certificate.

The certificate has now been created and resides in the "Issued certificates" folder. Next , you need to download and install the certificate:

1. Open http://<*MSFT CA hostname*>/certsrv.
2. Click **View the status of a pending certificate request**.
3. Click the certificate request.
4. Click the certificate in order to install it.

In order to let the ADAM service use the certificate, you need to put the certificate in the ADAM service's personal store:

1. From the Start menu, choose **Run**. Type **mmc**. This opens the managment console.
2. Click **File \ Add/Remove snap-in**.
3. Click **Add** and choose **Certificates**.
4. Chose **Service account**.
5. Choose **Local computer**.
6. Choose your ADAM instance service.
7. Add a new Certificate snap-in, but this time choose **My user account** instead of Service account.
8. Click **Close** and click **Ok**.
9. In the Certificates - Current user-tree, open the **Personal** folder.
10. Select the certificate and copy it into the same location under "Certificates - *adam instance name*".

In order to grant Read permission on the server authentication certificate to the Network service account, complete these steps:

1. Navigate to this default directory where the installed or imported certificates are stored - C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys.

2. Right-click the appropriate server authentication certificate. Click **Properties**.
3. Click the **Security** tab. Click **Edit**.
4. In the **Permissions** dialog box, click **Add**.
5. In the **Select Users, Computers, or Groups** dialog box, enter **Network Service.** Click **OK**.
6. Restart your ADAM instance.

More information can be found in Appendix A: Configuring LDAP over SSL Requirements for AD LDS.

Next, upload the certificate of the CA that issued the certificate to the ADAM/AD LDS machine as a CUCM directory trust.

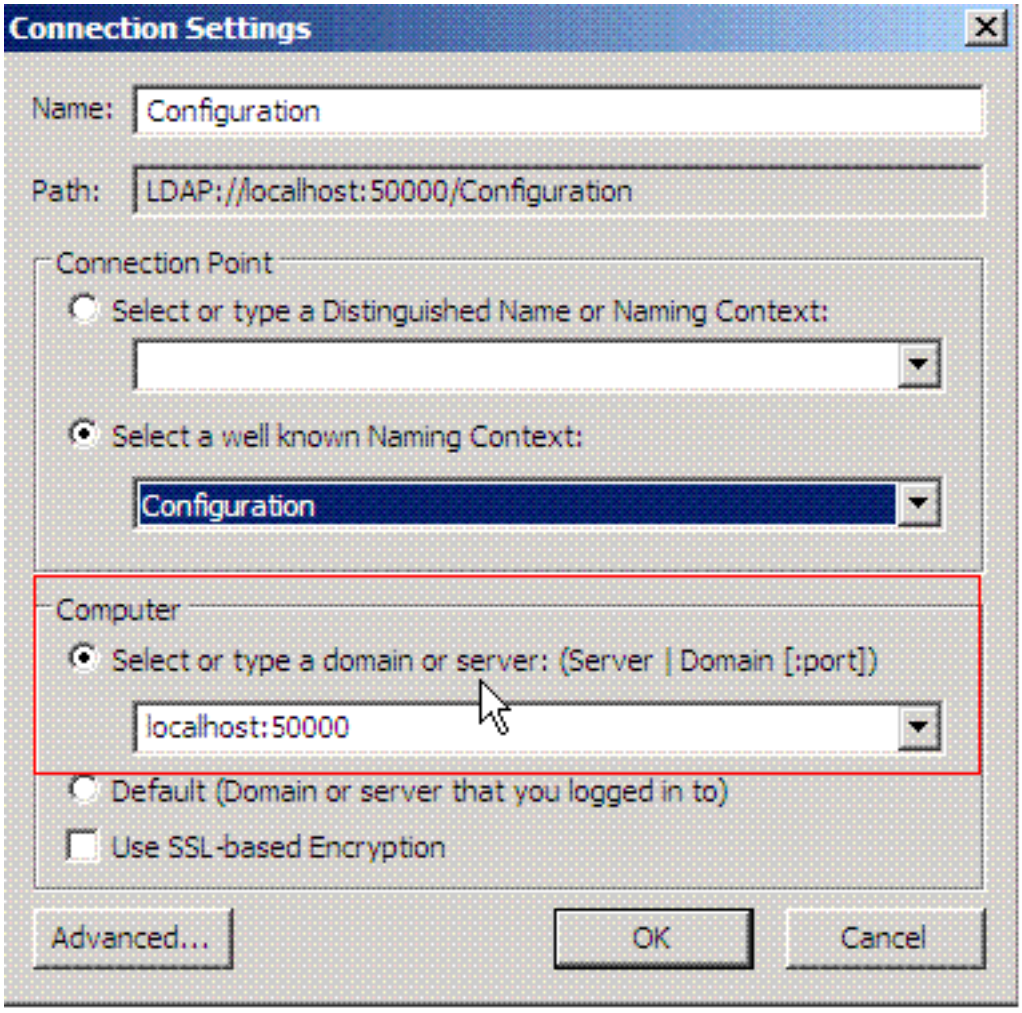
Refer to the Cisco Unified Communications Operations System Administration Guide for additional details.

Choose the checkbox in order to use SSL in LDAP Directory page and LDAP Authentication page.

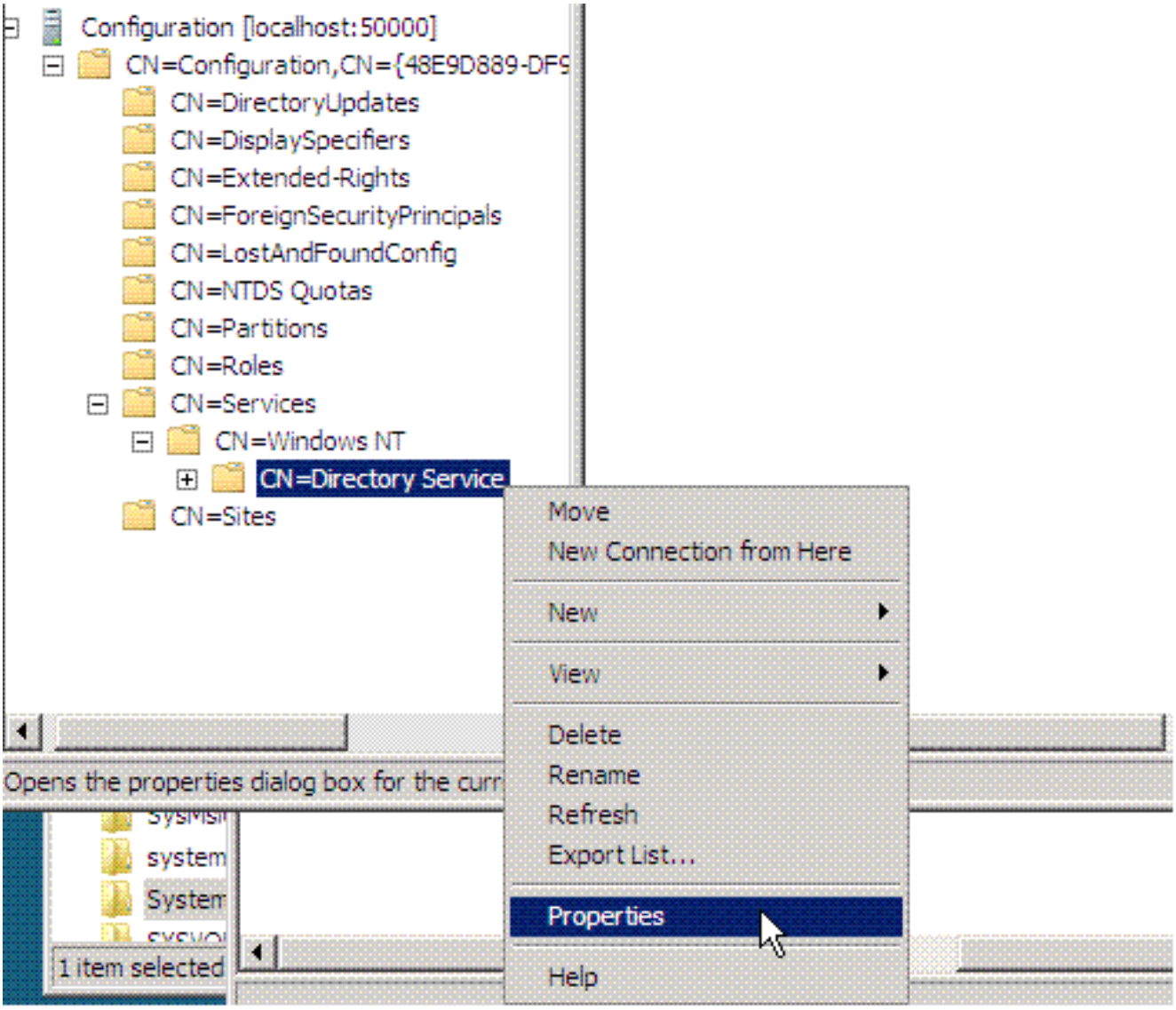
Enter 50001 (in this example) for the LDAP port, which is the SSL port number given when you installed the ADAM/AD LDS instance.

In order to disable the SSL requirement for bind redirection, complete these steps:

1. Click **Start**, point to **Administrative Tools**, and click **ADSI Edit**.
2. On the Action menu, choose **Connect to**.
3. In the Computer field, enter **localhost:50000** (this is theADAM host and port.).



4. In the Connection Point section, click the **Select a well-known Naming Context** radio button. From the drop-down list, choose **Configuration**. Click **OK**.
5. In the console tree, browse to this container object in the configuration partition: CN=Directory Service,CN=Windows NT,CN=Services.
6. Right-click **CN=Directory Service** and choose **Properties**.

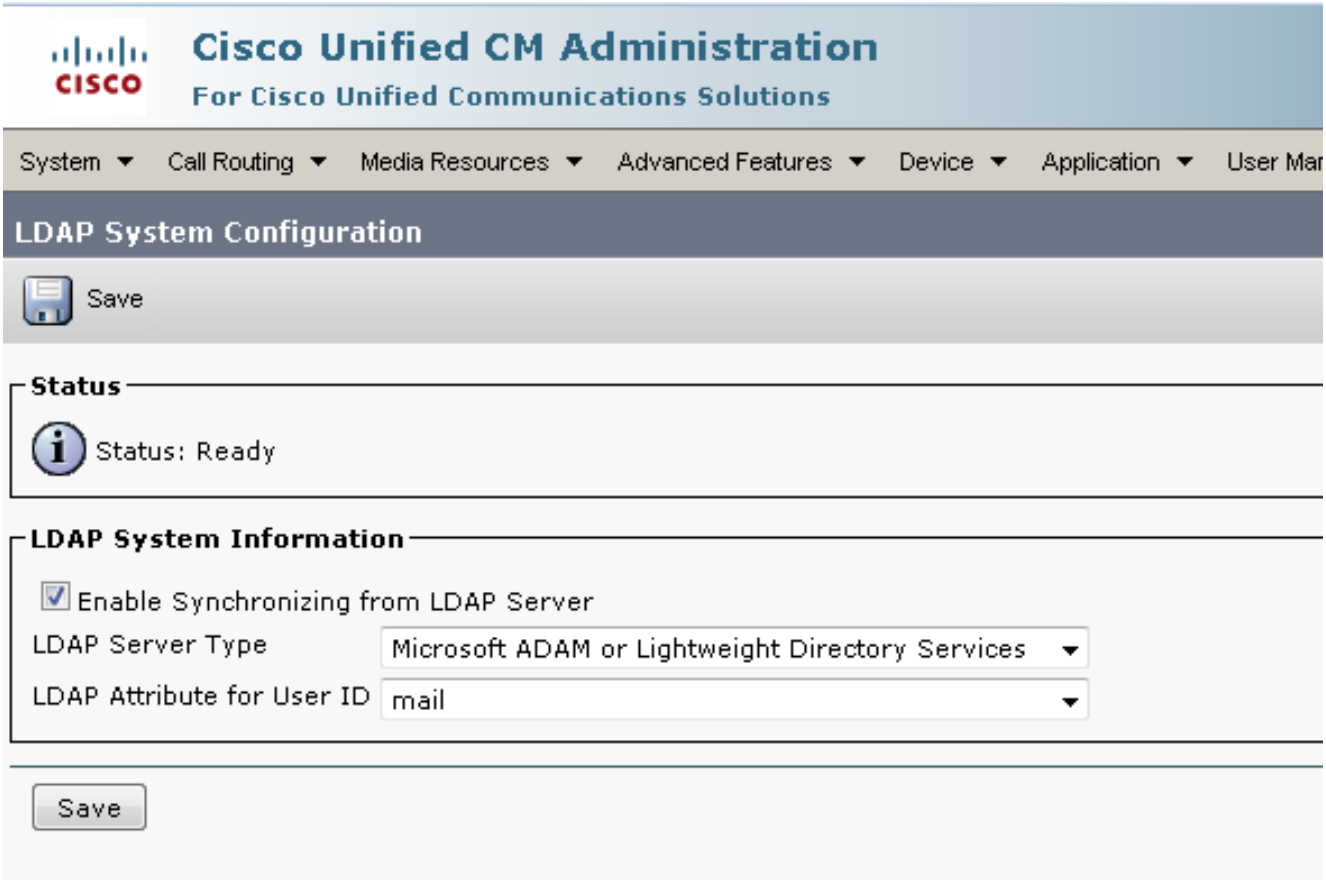


7. In Attributes, click **msDS-Other-Settings**. Click **Edit**.
8. In Values, click **RequireSecureProxyBind=1** and then click **Remove**.
9. In Value to add, enter **RequireSecureProxyBind=0**, click **Add**, and then click **OK**.
10. Restart AD LDS for the changes to take effect.

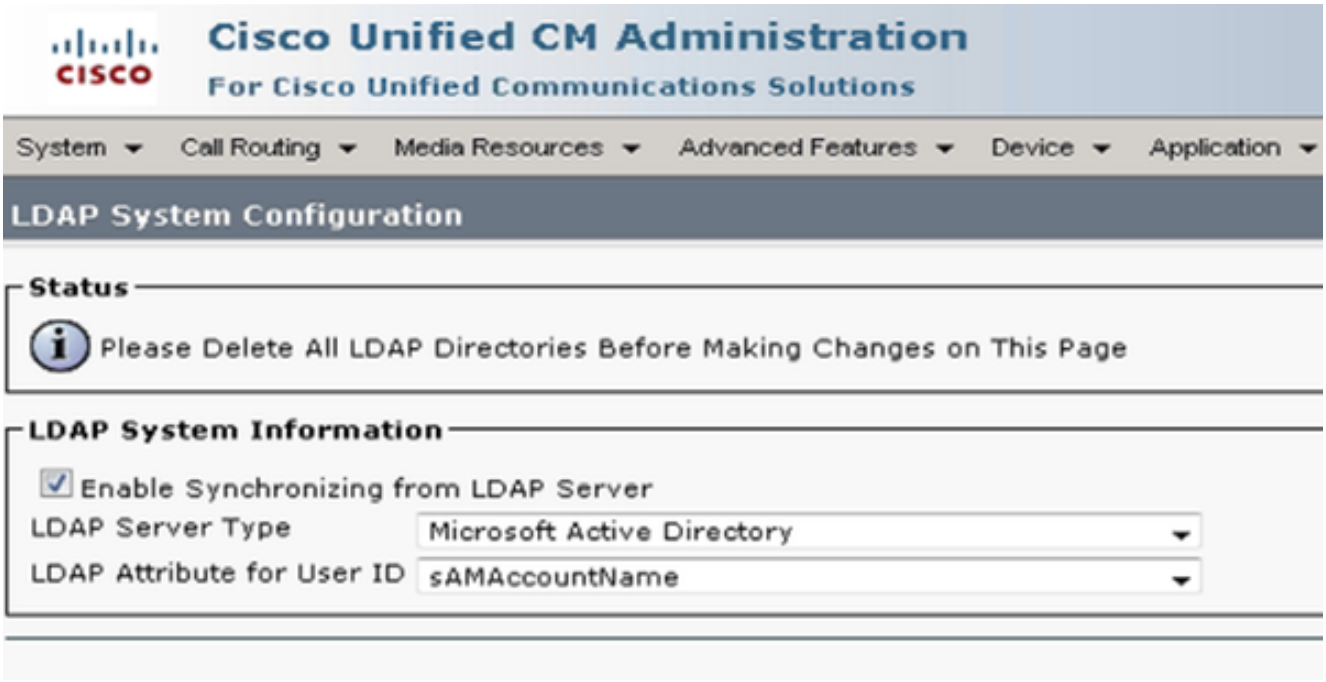
Configure CUCM

ADAM/AD LDS synchronization and authentication is supported in CUCM Version 9.1(2) and later.

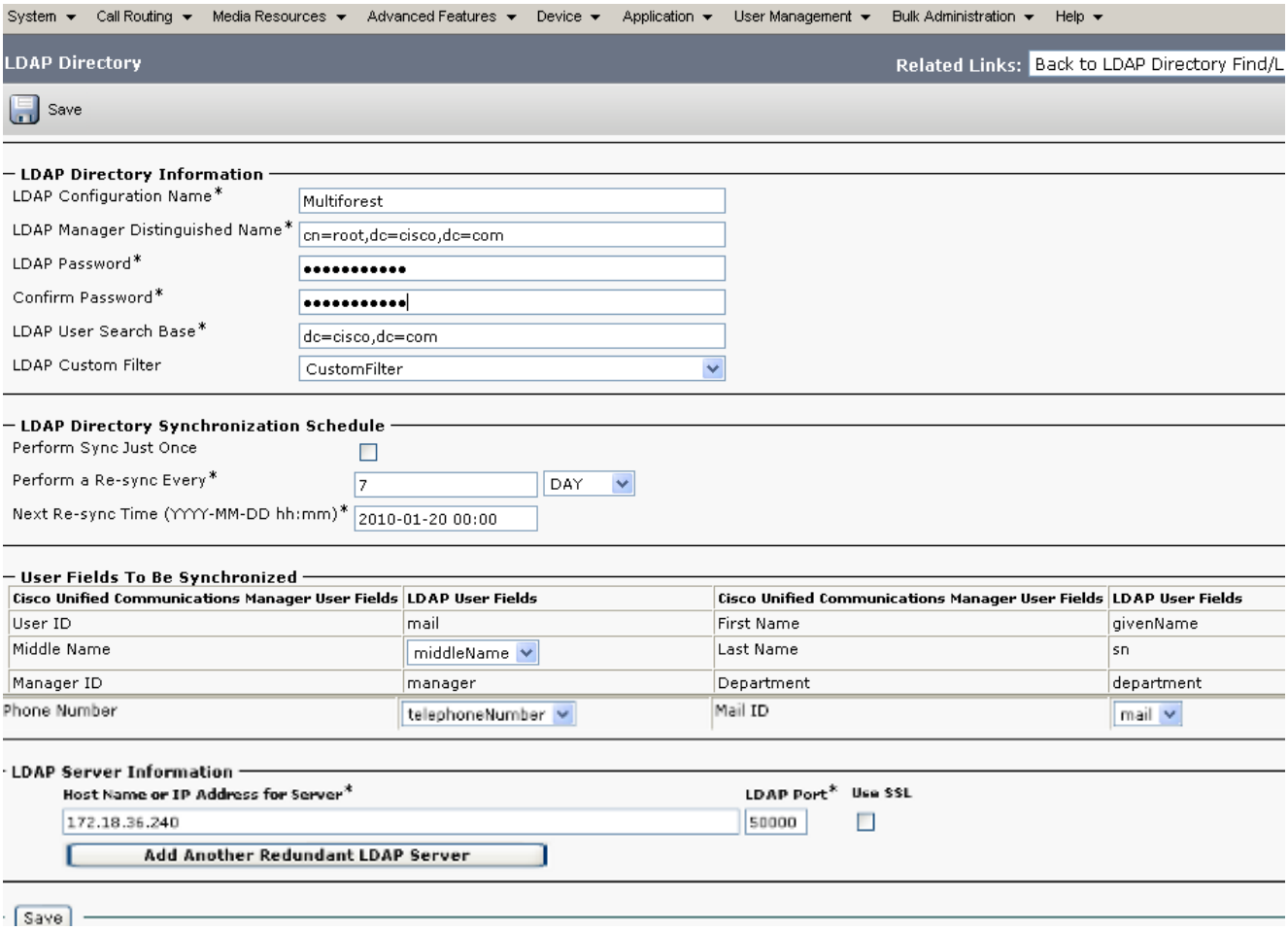
1. Choose **System > LDAP > LDAP System**.
2. Select Microsoft ADAM or Lightweight Directory Services.
3. You can choose any of these LDAP userid attributes: mail, employee Number, or telephone Number. uid is only used with standalone ADAM/AD LDS and not with AD multi-forest support.



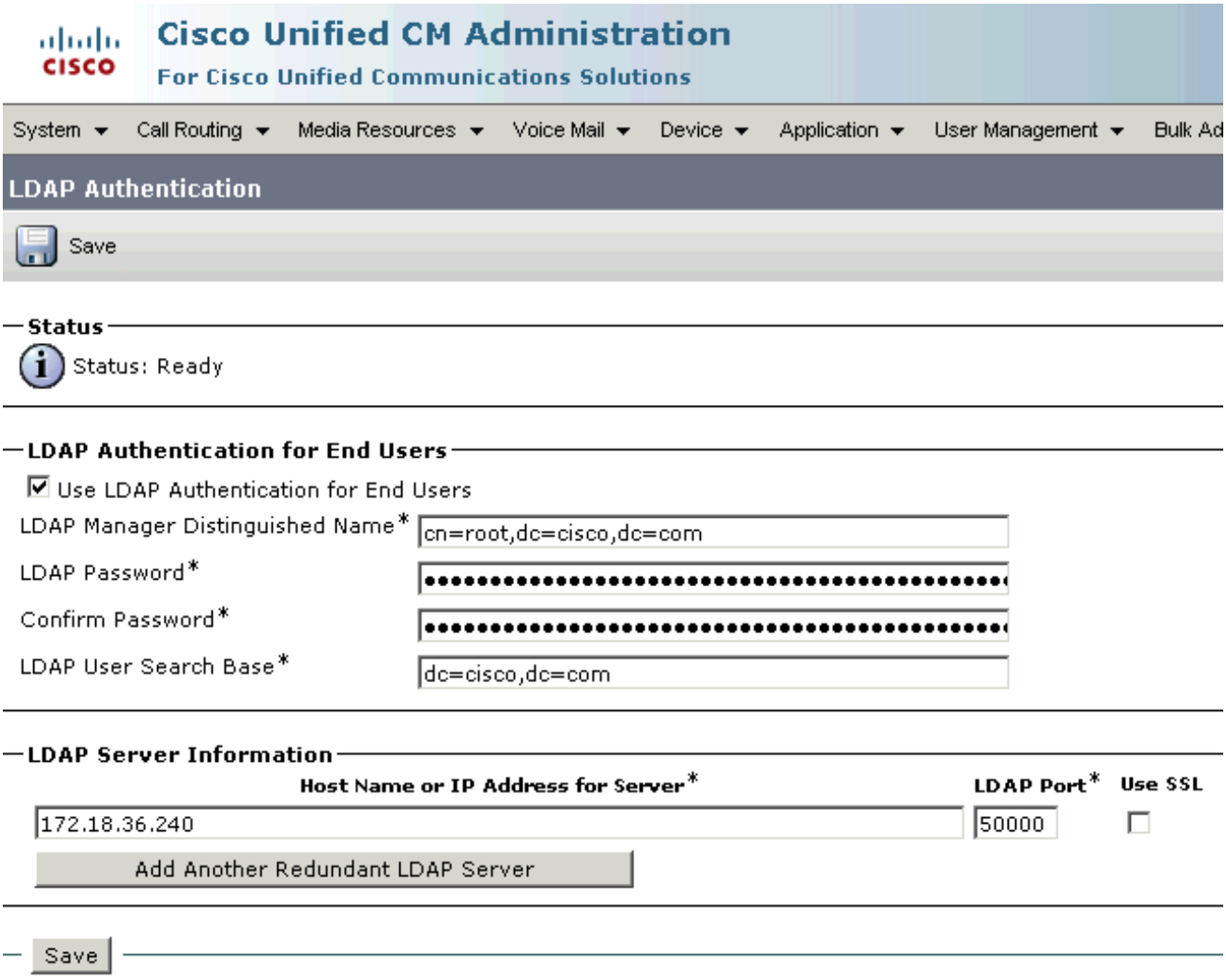
Currently, for LDAP Server type "Microsoft ADAM or Lightweight Directory Services" mode, samAccountName is not included in the LDAP Attribute for Userid drop-down . The reason is that it is not an attribute supported with standalone ADAM/AD LDS. If the CUCM UserID mapped to sAMAccountName needs to be used then that agreement should be configured as
AD.



4. Configure LDAP synchronization with the credentials of the user created in AD LDS.



5. Configure LDAP authentication with the credentials of the user created in AD LDS.

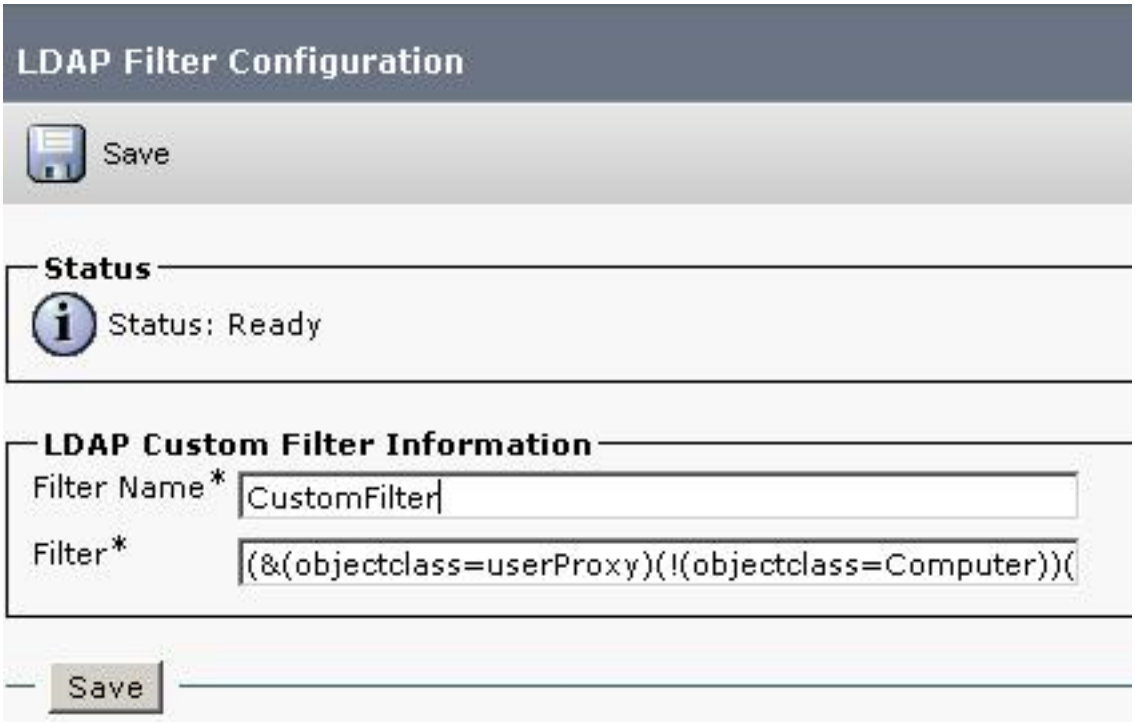
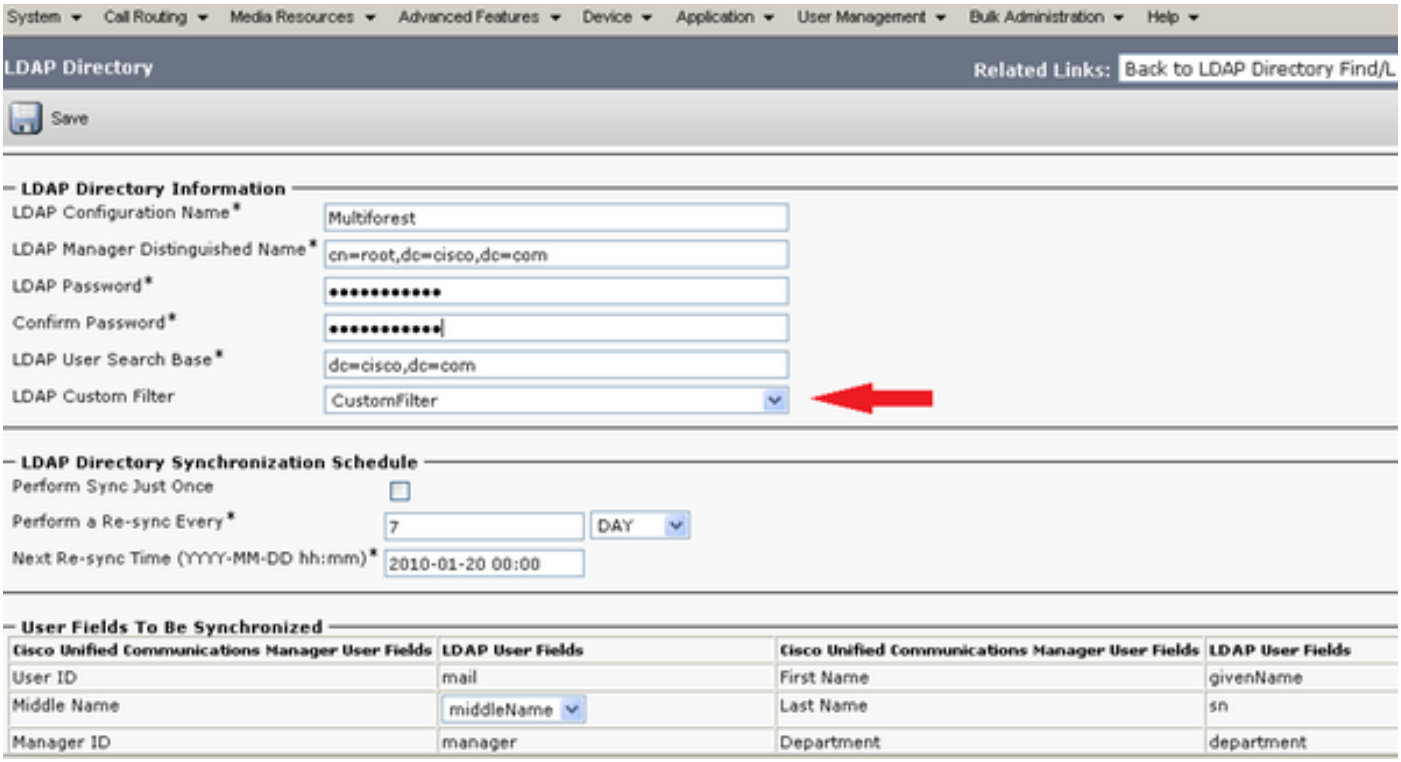


LDAP Filters in CUCM

The object class User is no longer used. Therefore, the LDAP filter needs to be changed to use userProxy instead of User.

The default filter is:
(&(objectclass=user)(!(objectclass=Computer))(!(msDS-UserAccountDisabled=TRUE)))

In order to modify this filter, log in to CCMAdmin with a web browser and choose the LDAP Custom Filter option from the LDAP configuration menu.



This filter is used in the LDAP directory page while configuring LDAP the synchronization agreement as shown in the previous figure.