

Unified CM 8.0(1) Multiple Forest Integration with Microsoft ADAM/LDS





Contents

| | |
|--|----|
| Requirements | 3 |
| Definitions | 3 |
| Preface..... | 4 |
| Overview..... | 5 |
| Active Directory multiple forest support scenario in Unified CM | 7 |
| Domain trust relationship | 8 |
| Install AD LDS..... | 14 |
| Install the instance for multiple-forest support | 16 |
| Copy the schema from each domain to ADAM | 22 |
| Extend the AD LDS schema with the user-proxy objects | 27 |
| Import the users from AD DC to AD LDS | 29 |
| Creating the user in AD LDS for Unified CM synchronization and authentication..... | 32 |
| Configuring Bind Redirection | 39 |
| Configuring Unified CM..... | 40 |
| Creating a Custom LDAP filter in Unified CM..... | 44 |



Requirements

This White paper assumes that the reader understands the following:

1. Customer has knowledge of deploying and configuring Cisco Unified Communications Manager directory integration.
2. Customer is responsible for deploying, configuring, and maintaining Microsoft Active Directory Application Mode 2003 or Microsoft Active Directory Lightweight Directory Services 2008.
3. Customer has Cisco Unified Communications Manager, Release 8.0(1), or later.
4. Number of User Accounts to be synchronized does not exceed 60,000 accounts per Unified CM Publisher. When more than 60,000 accounts need to be synchronized, the IP Phone Services SDK must be used to provide a custom directory. Refer to the Cisco Developer Network for additional details: <http://developer.cisco.com/web/ipps/home>
5. Customer uses Microsoft Active Directory Application Mode 2003 or Lightweight Directory Services 2008.

Definitions

| Word | Definition |
|------------|---|
| AD | Microsoft Active Directory |
| AD DS | Microsoft Active Directory Domain Service |
| AD LDS | Microsoft Active Directory Lightweight Directory Services |
| ADAM | Microsoft Active Directory Application Mode |
| DirSync | Cisco Unified CM Directory Integration Service |
| LDAP | Lightweight Directory Application Protocol |
| Unified CM | Cisco Unified Communications Manager |
| SSO | Single Sign On |



Preface

Microsoft Active Directory Lightweight Directory Service (AD LDS), formerly known as Active Directory Application Mode, can be used to provide directory services for directory-enabled applications. Instead of using your organization's Active Directory Domain Service (AD DS) database 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 to support the application configuration and directory data (AD LDS). Using AD LDS, you can reduce the overhead associated with Active Directory replication. You do not have to extend the Active Directory schema 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.

Many differences exist between ADAM and Active Directory. ADAM can only deliver some of the Active Directory (AD) functions, as shown in the figure that follows.

| Active Directory | | | ADAM | |
|---------------------------------|-----------------------|-----------------|---------------------------------|--|
| Replication | Kerberos KDC | | Replication | |
| Directory Service (DSA) | MAPI Support | | Directory Service (DSA) | |
| Extensible Storage Engine (ESE) | Group Policy (SYSVOL) | | Extensible Storage Engine (ESE) | |
| LDAP | Global Catalog | DNS SRV Records | LDAP | |



Overview

This document explains the mechanisms that allow Cisco Unified Communications Manager (Unified CM), or any other Cisco products that use DirSync, to get user information and perform authentication from different AD forests, that can exist in different forests. To achieve this objective, we use ADAM, which can synchronize its user database with different AD Domain Controllers or other LDAP sources.

ADAM can create a database of users and store the user details. Single Sign On (SSO) functionalities are desired to avoid end users having to maintain different sets of credentials in different systems; therefore, ADAM bind redirection will be 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, may force you to avoid Active Directory, making ADAM a necessary choice.

A special user proxy object in ADAM maps to a regular Active Directory user account. The user proxy does not have an actual password stored in the ADAM object itself. When performing its normal bind operation, the application checks the ID locally but checks the password against Active Directory under the covers, as Figure 1 illustrates. The application does not need to be aware of this Active Directory interaction.

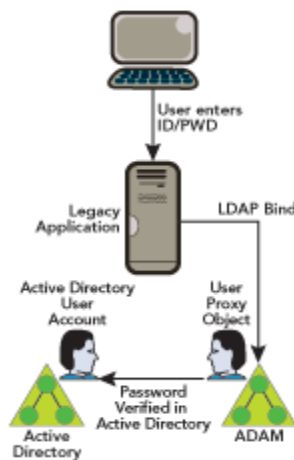


Figure 1: ADAM User Proxy Password Authentication



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 Active Directory.

ADAM bind redirection occurs when a bind to ADAM is attempted using a special object called a proxy object. A proxy object is an object in ADAM that represents a security principal in Active Directory. Each proxy object in ADAM contains the SID of a user in Active Directory. 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 Active Directory for authentication. A proxy object in ADAM does not store a password, and users cannot change their Active Directory 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 to present the password to Active Directory.

You can find more information about bind redirection at the following URL:

<http://technet.microsoft.com/en-us/library/cc758386%28WS.10%29.aspx>

Note

- The requirement for SSL when using bind redirection should not be disabled.



Active Directory multiple forest support scenario in Unified CM

For the purpose of explaining the method, we imagine a scenario where Cisco Systems (Forest 2) has acquired two other companies: Tandberg (Forest 3) and WebEx (Forest 1). In the migration phase, we integrate the Active Directory structure of each company, which allows the deployment of a single Cisco Unified Communications cluster.

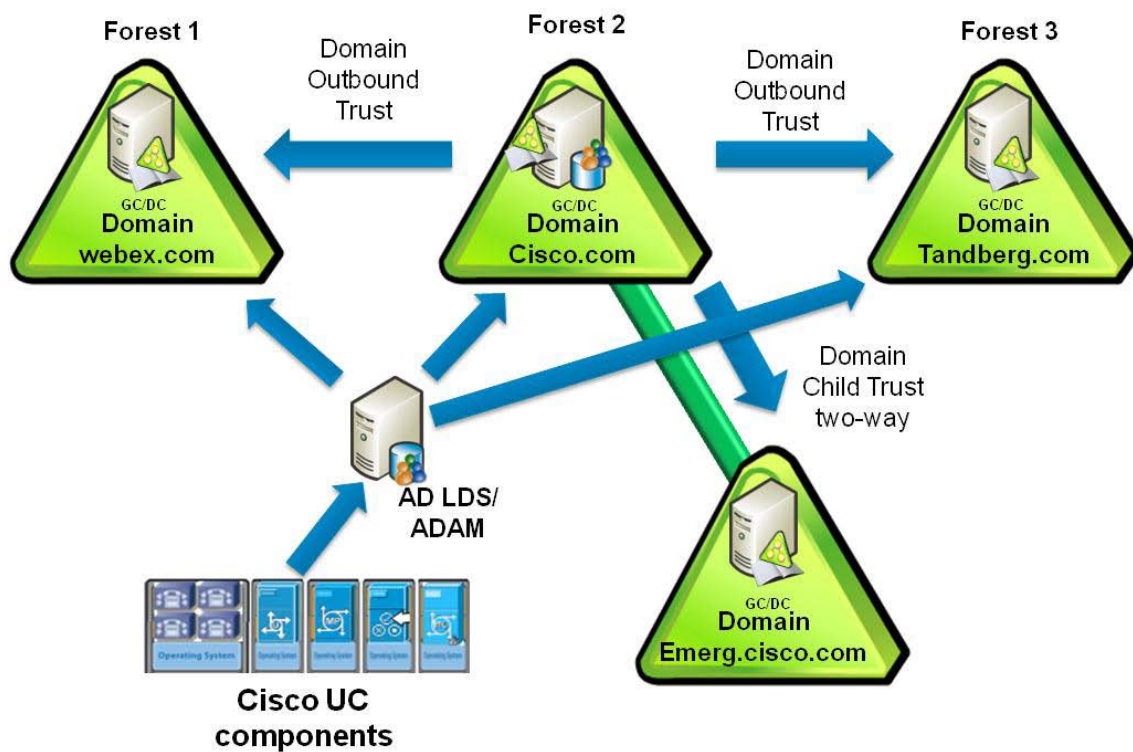


Figure 2: Example Multi-Forest Scenario

In our example, company Cisco (Forest 2) has two domains: Forest root domain called CISCO (dns cisco.com), and a sub domain called EMERG (dns emerg.cisco.com). Both 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; in fact, any machine anywhere in one of the three forests can be used. The DNS infrastructure must be in place such that domains in one forest can communicate with domains in other forests and can establish the appropriate trust relationships and validations between the forests.

Domain trust relationship

For the authentication of the users to succeed, you need to have a trust between the domain where the ADAM instance is hosted and the other domain(s) that host 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 host the user accounts). Thus, the ADAM instance can forward the authentication requests to DC's in those account domains.

Furthermore, you need a user account from both account domains that has access to all attributes of all user accounts in the domain. ADAMSync uses this account to synchronize the Account Domain users to ADAM.

Finally, the machine that runs ADAM must be able to find all domains (DNS), find domain controllers in both domains (using DNS), and connect to these Domain Controllers.

Use the following steps to set up the inter trust relationships:

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

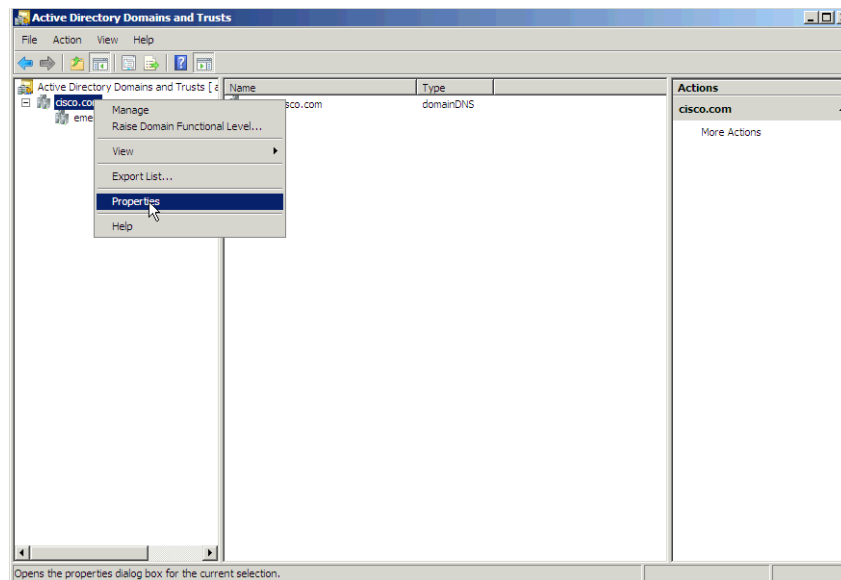


Figure 3: Active Directory Domains and Trusts Window

Note: The domain functional level and the forest functional level should specify 2003 or higher.



2. Go to the Trusts tab, and click **New Trust**.

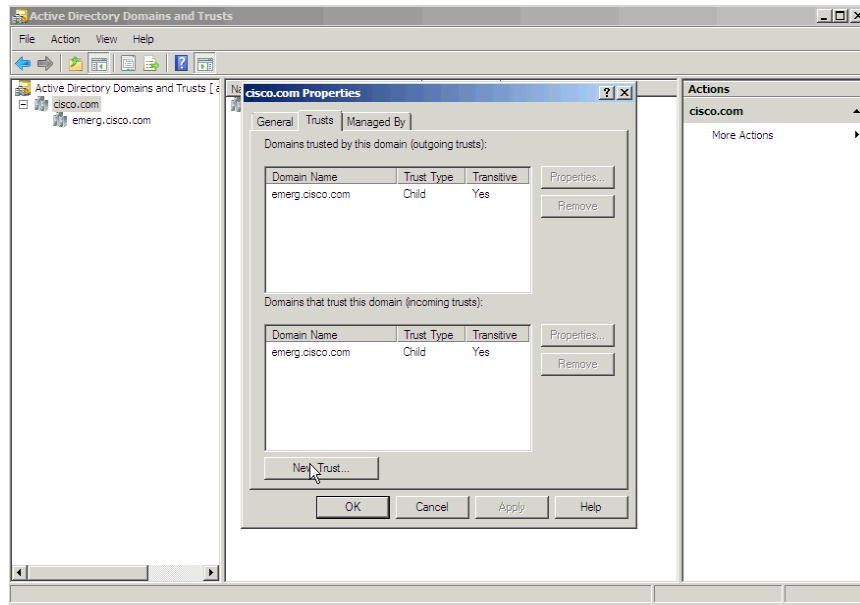


Figure 4: Trusts Tab

3. Follow the wizard and provide the name of the domain with which you want to establish the trust; then, click **Next**.

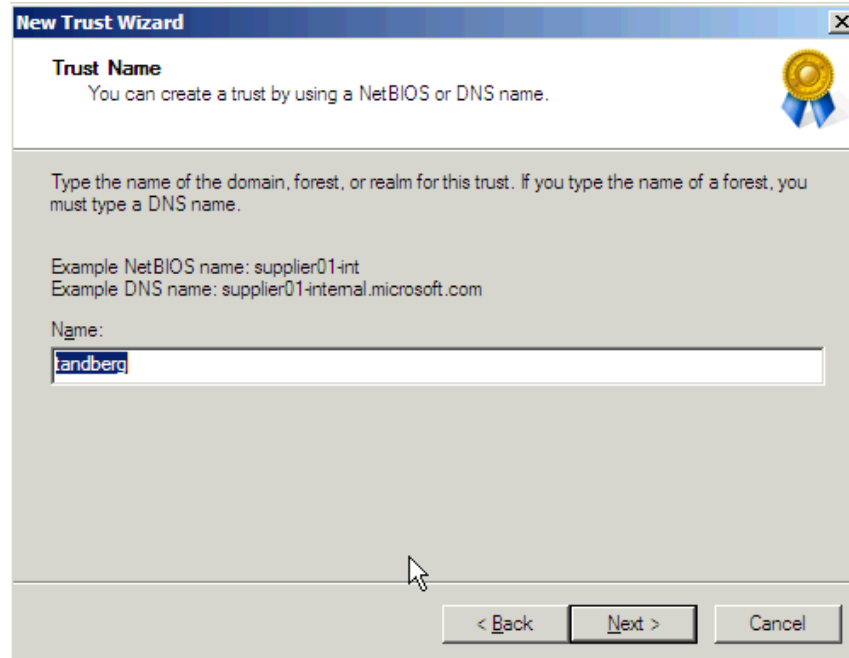


Figure 5: New Trust Wizard Name Entry

In the Trust Type window, choose Forest trust; then, click **Next**.

Cisco Public

Copyright © 2010 Cisco Systems, Inc. All rights reserved.

Page 9 of 44

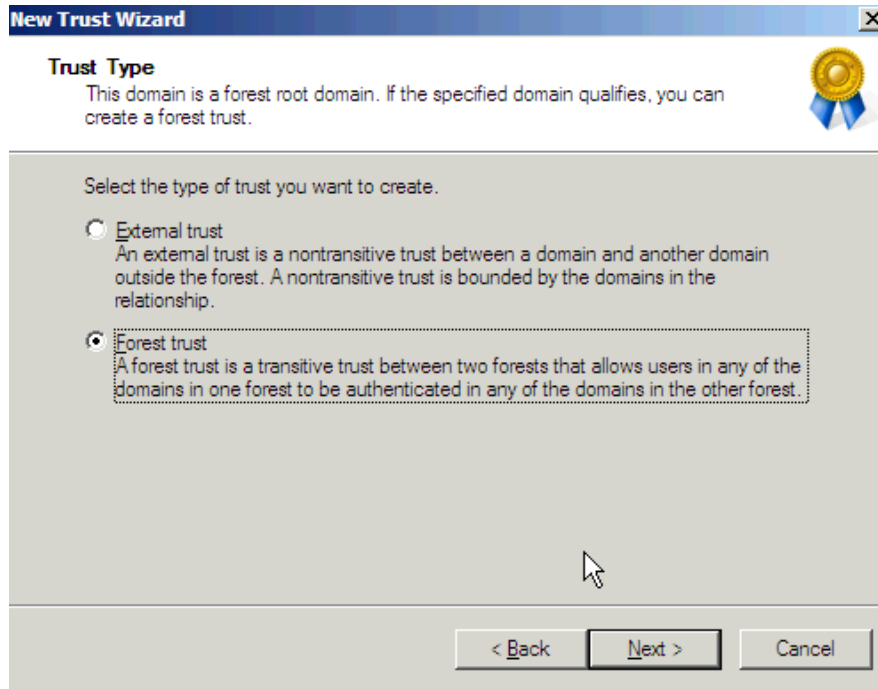


Figure 6: Trust Type

4. In the Direction of Trust window, choose One-way: outgoing (required); then, click **Next**.

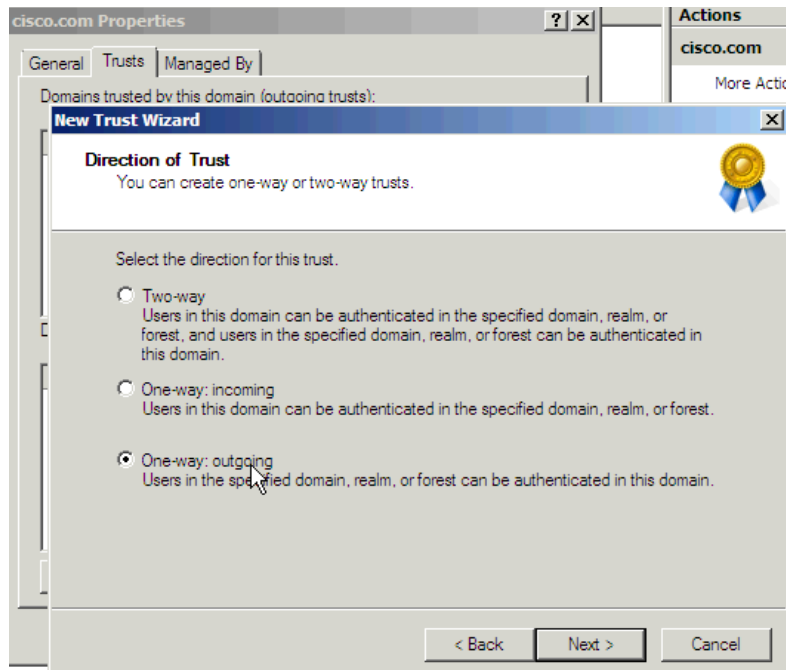


Figure 7: Direction of Trust

5. In the Size of Trust window, allow the wizard to configure both domains. To do so, choose Both this domain and the specified domain; then, click **Next**.

Cisco Public

Copyright © 2010 Cisco Systems, Inc. All rights reserved.

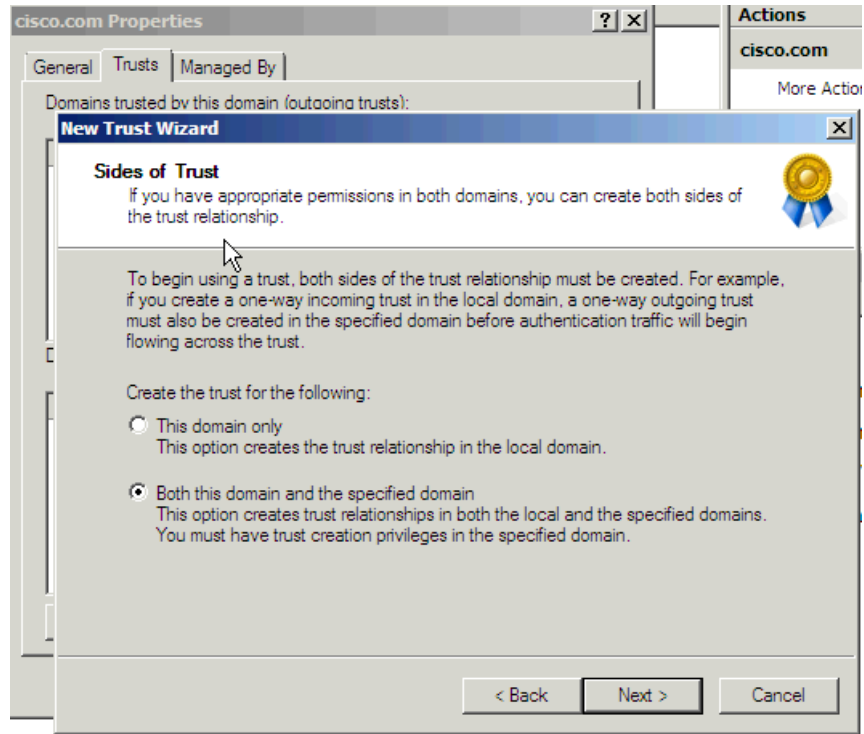


Figure 8: Sides of Trust

6. In the User Name and Password window, provide the credentials for the other domain; then, click **Next**.

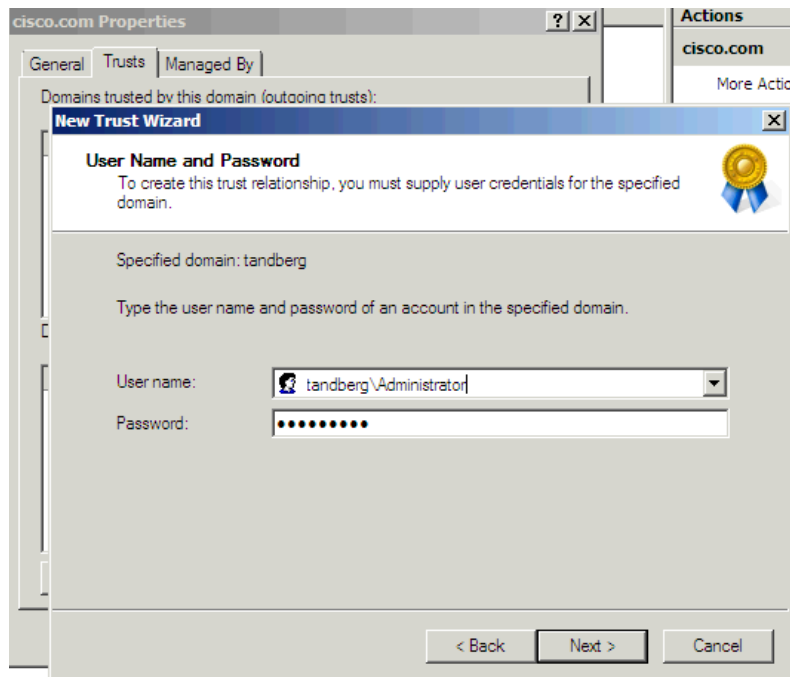


Figure 9: User Name and Password



7. In the **Outgoing Trust Authentication Level—Local Forest** window, choose **Forest-wide authentication**; then, click **Next**.

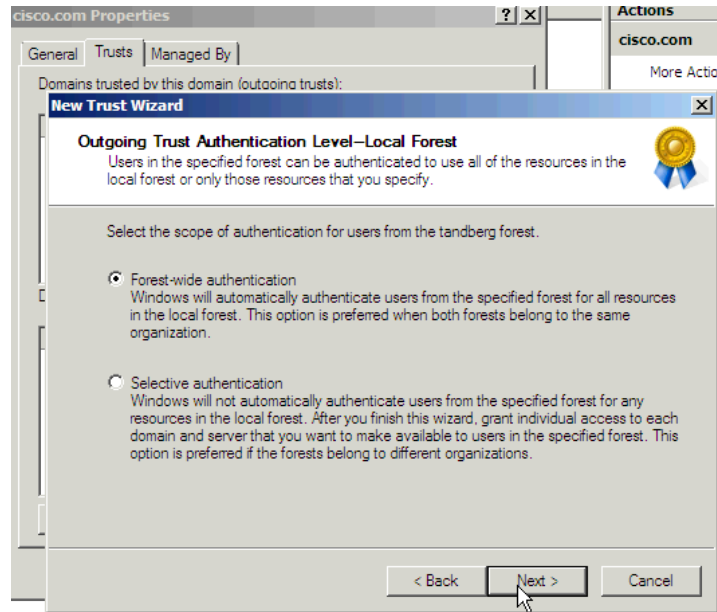


Figure 10: Outgoing Trust Authentication Level—Local Forest

8. In the **Confirm Outgoing Trust** window, choose “**Yes, Confirm the outgoing trust**” then, click **Next**.

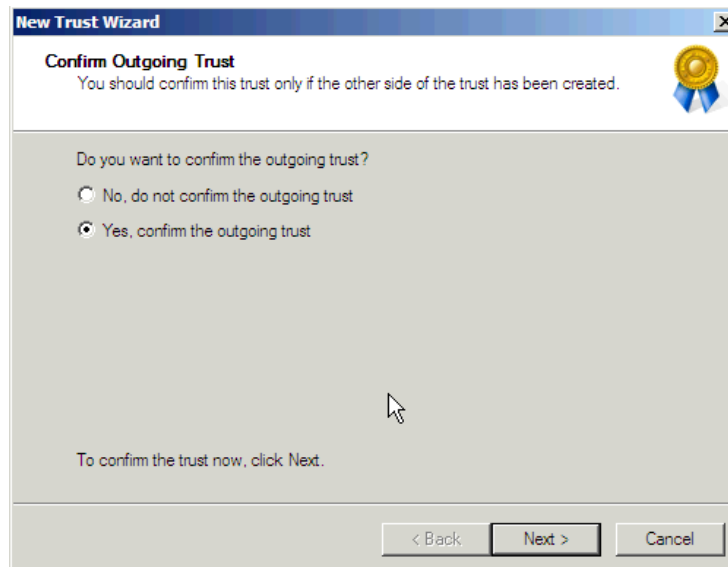


Figure 11: Confirm Outgoing Trust



The following displays after you run this process for both the Tandberg and WebEx domains. The emerg domain displays by default, because it is a child domain.

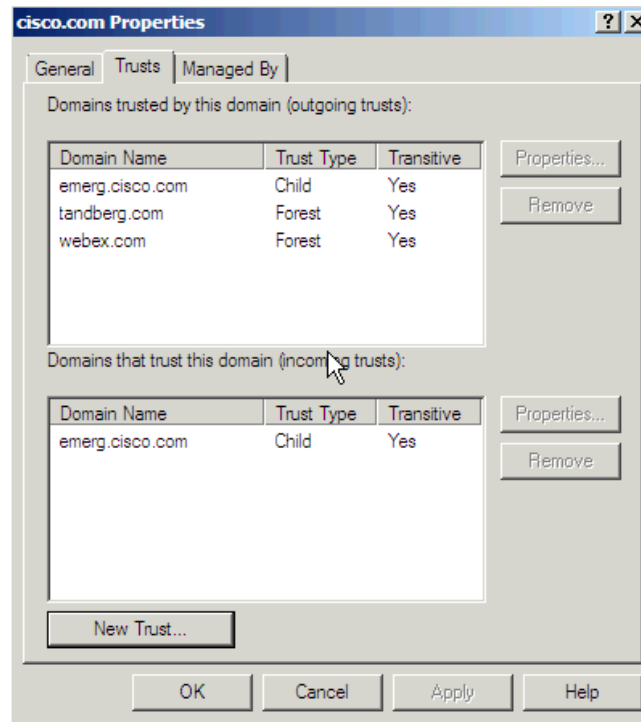


Figure 12: Properties Window, Trusts Tab



Install AD LDS

1. Open Server Manager, click on Roles, and select add New.

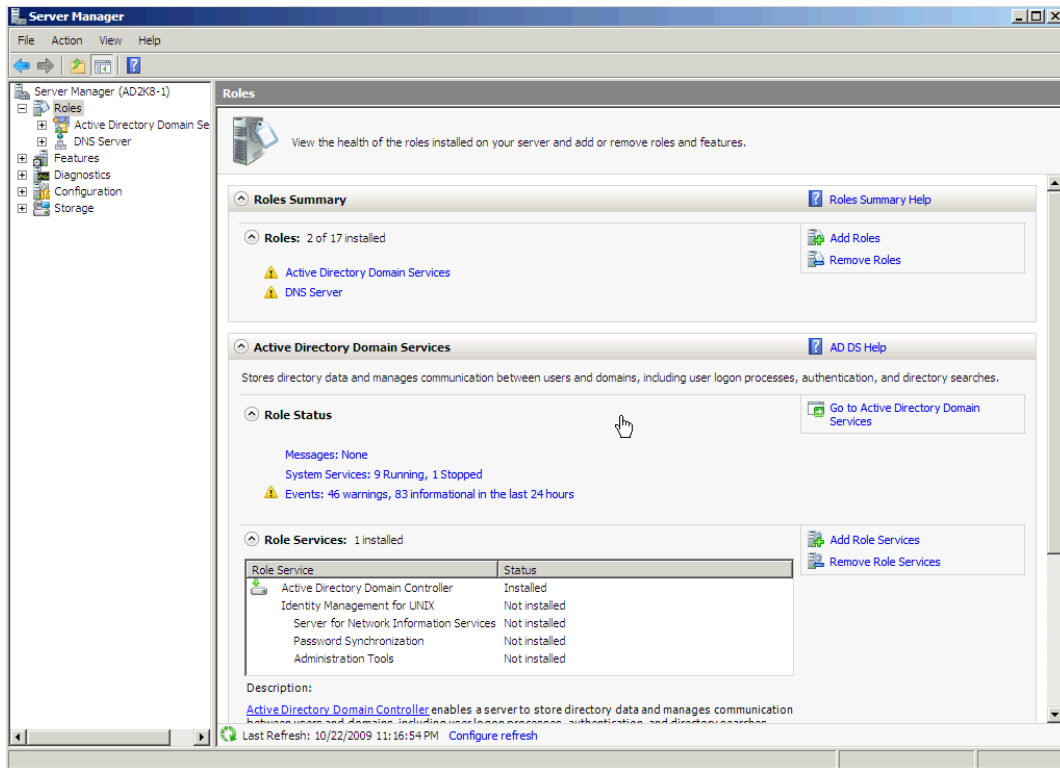


Figure 13: Server Manager



2. In the Select Server Roles window, choose Active Directory Lightweight Directory Services; then, click **Next**.

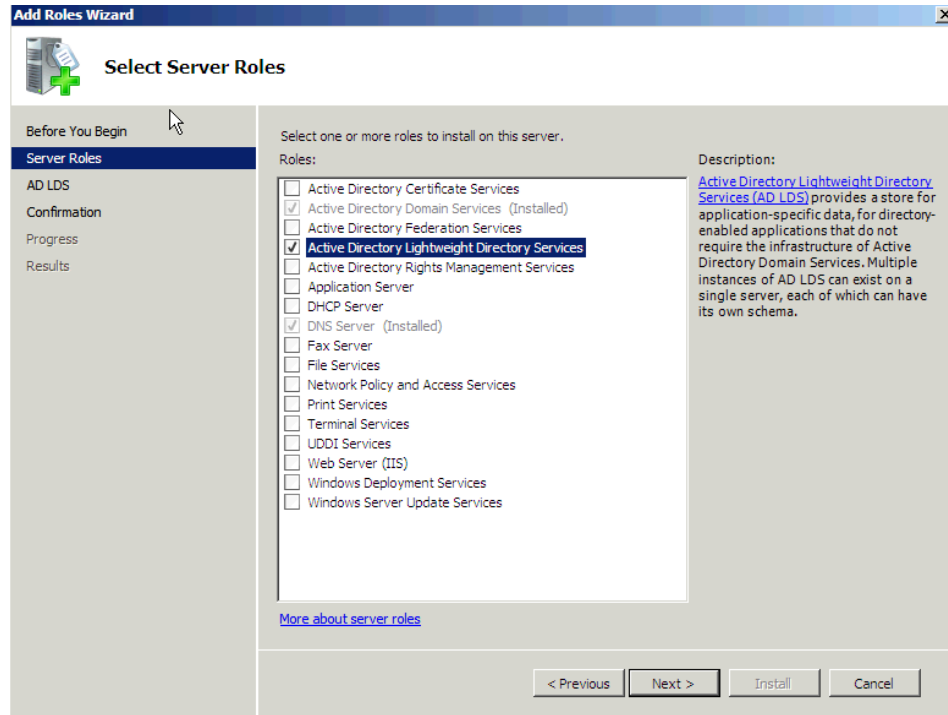


Figure 14: Select Server Roles

AD LDS services installation

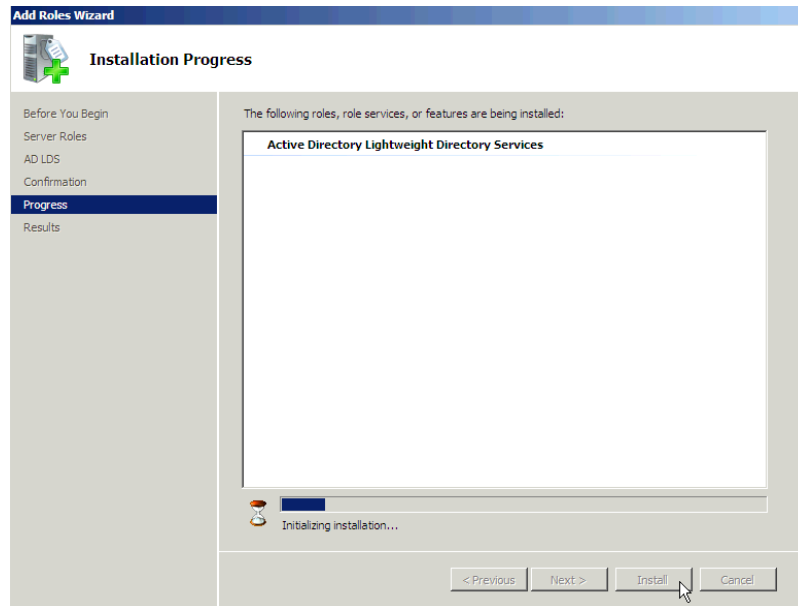


Figure 15: Installation Progress



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/LDAP. If the system already has any kind of LDAP services running, however, it uses ports 50000/LDAP and 50001/LDAPS. Each instance has a pair of ports that increment based on the previous numbers used.

In some cases, due to a Microsoft bug, the ports are already in use by Microsoft DNS server and the instance wizard shows an error, which is not self explanatory. To fix this error, reserve the ports in the tcp/ip stack. If you find this problem, refer to the following document:

AD LDS service start fails with error "setup could not start the service..." + error code 8007041d
<http://support.microsoft.com/kb/959215>

In the Server Manager, select Roles and then AD LDS.

1. Select *Click here to create an AD LDS instance*.

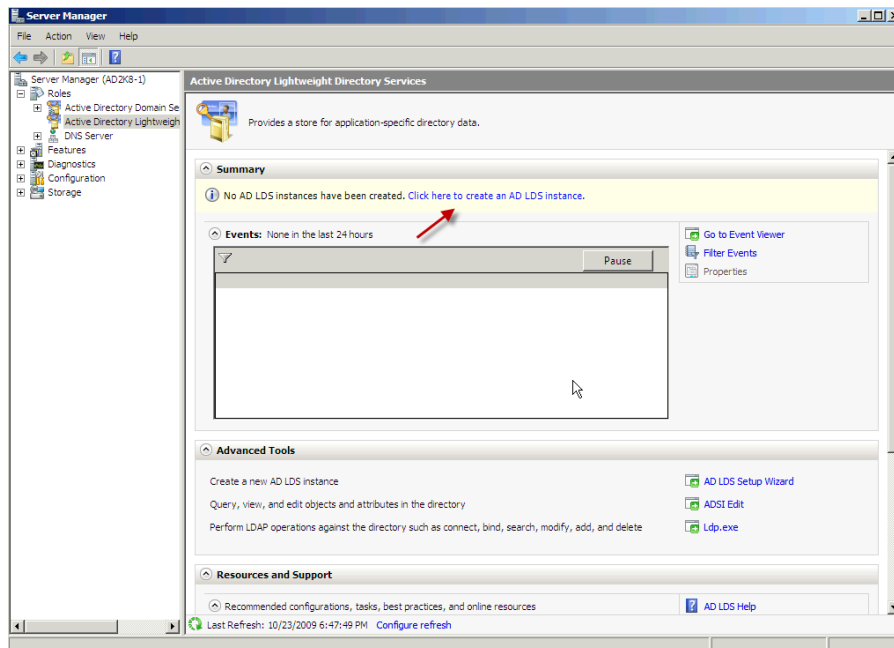


Figure 16: Active Directory Lightweight Directory Services Window



2. In the Setup Options window, choose *A unique instance*; then, click **Next**.

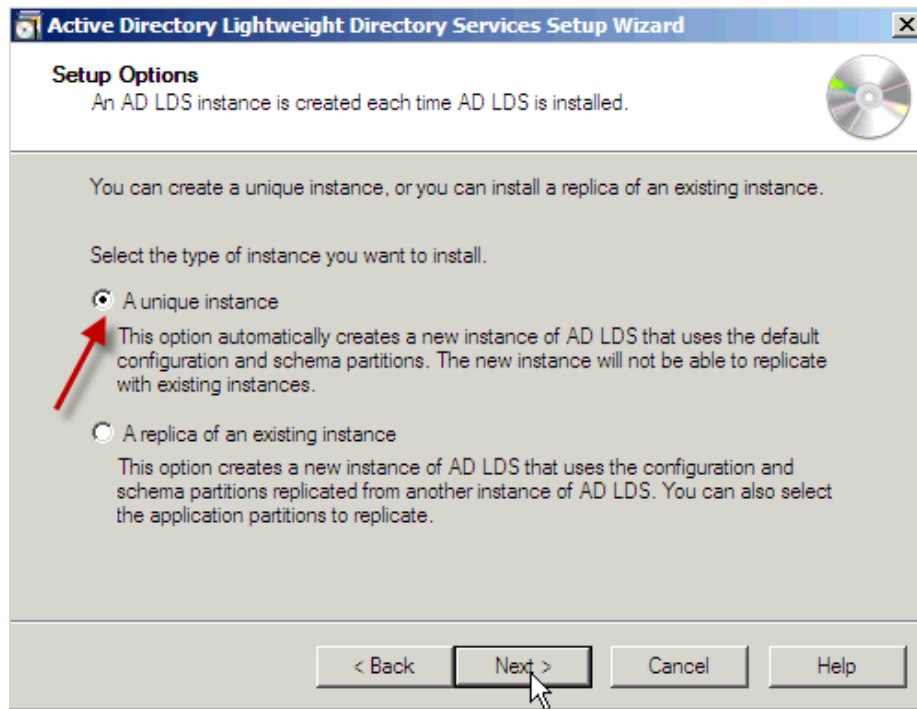


Figure 17: Setup Options Window

3. In the Instance Name window, provide the name of the instance. In our example, this is MultiForest. Click **Next**.

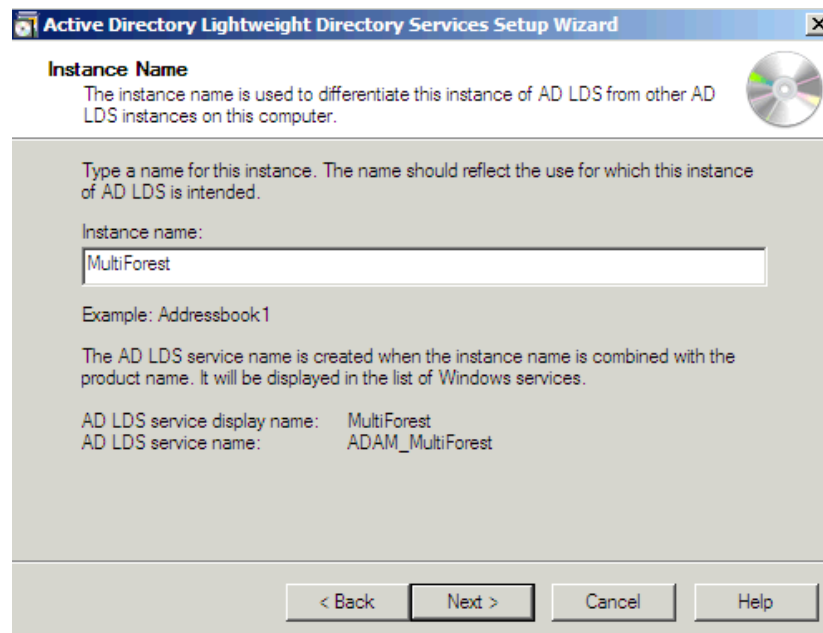


Figure 18: Instance Name Window



4. In the Ports window, choose the ports or allow the system to choose them for you. Click **Next**.

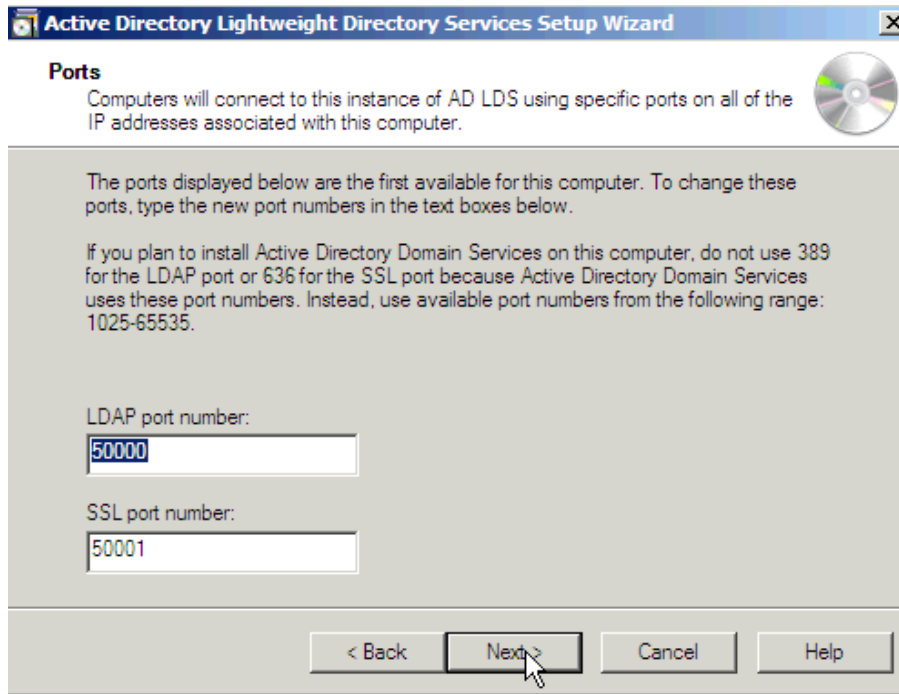


Figure 19: Ports Window



- In the Application Directory Partition window, provide a partition name for the instance. Do not provide a cn such as the one provided in the example of the wizard, because most of the time that will create an error in the Schemas. In our scenario, we choose the same partition as the Active directory domain controller that hosts AD LDS (dc=Cisco,dc=com). Click **Next**.

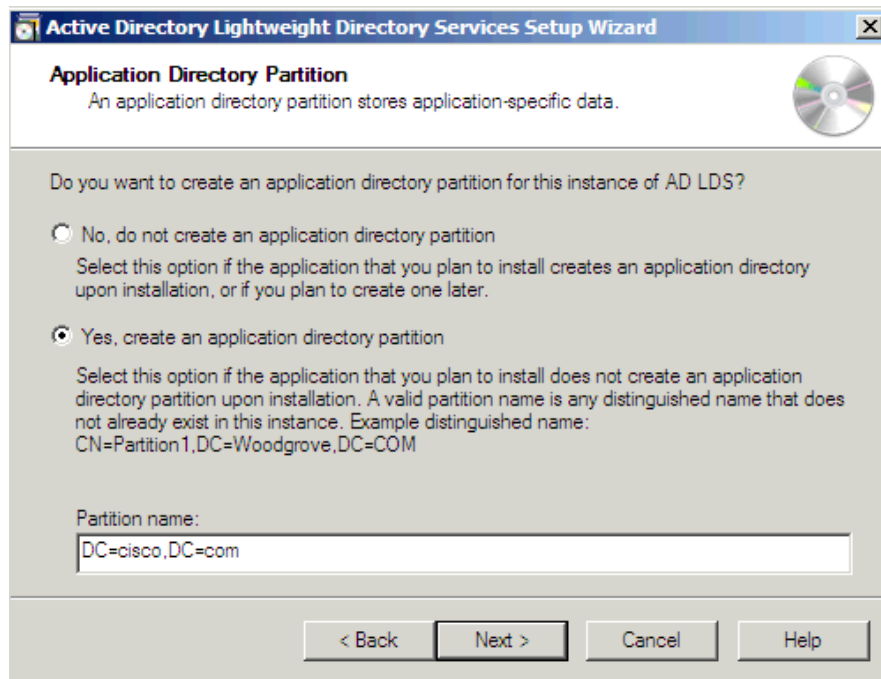


Figure 20: Application Directory Partition

- In the Service Account Selection window, provide an account to start the server.

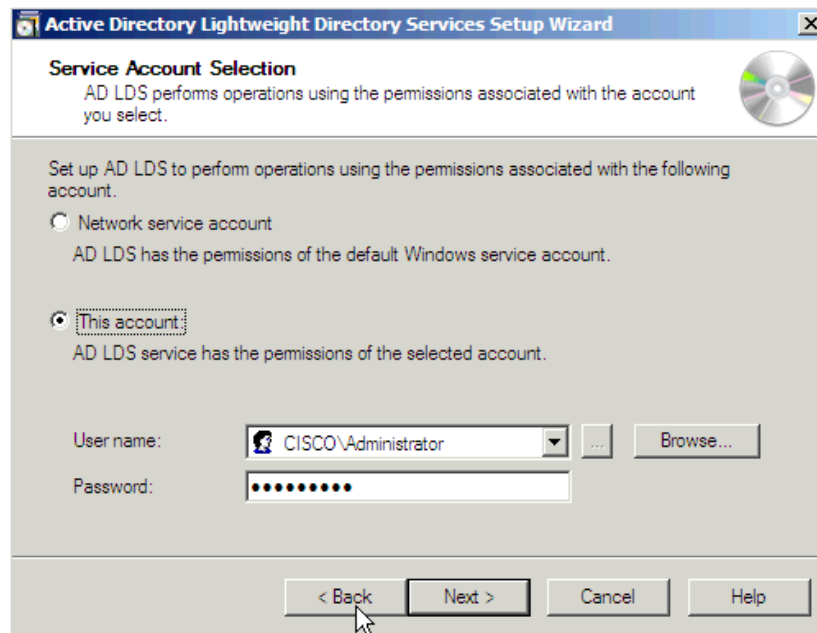


Figure 21: Service Account Selection



7. Provide the name of the user that has administrative permissions.

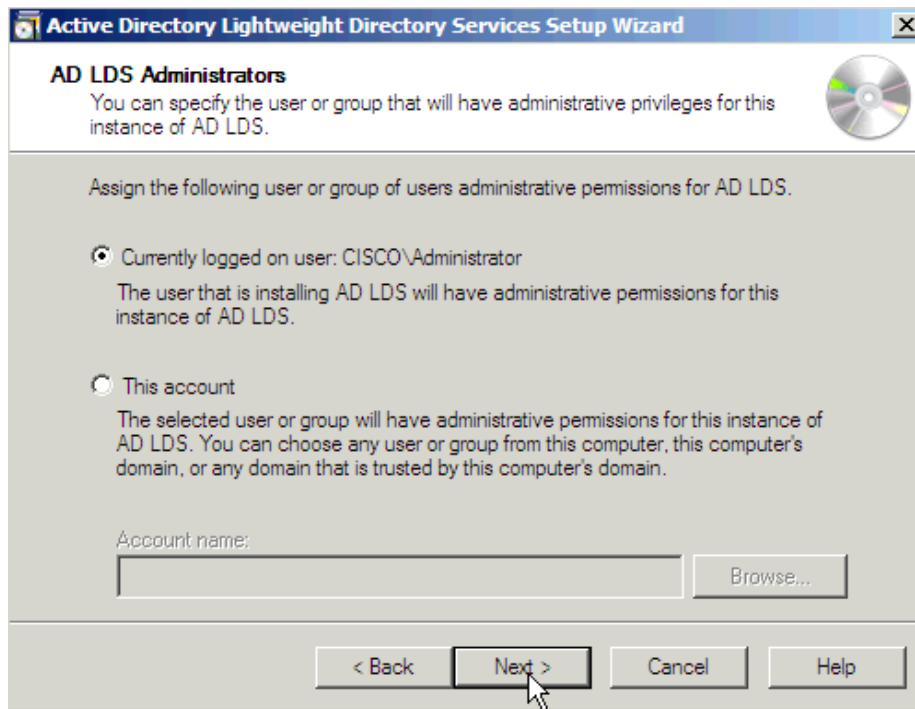


Figure 22: AD LDS Administrators



8. Import the highlighted default LDIF files to build the schema.

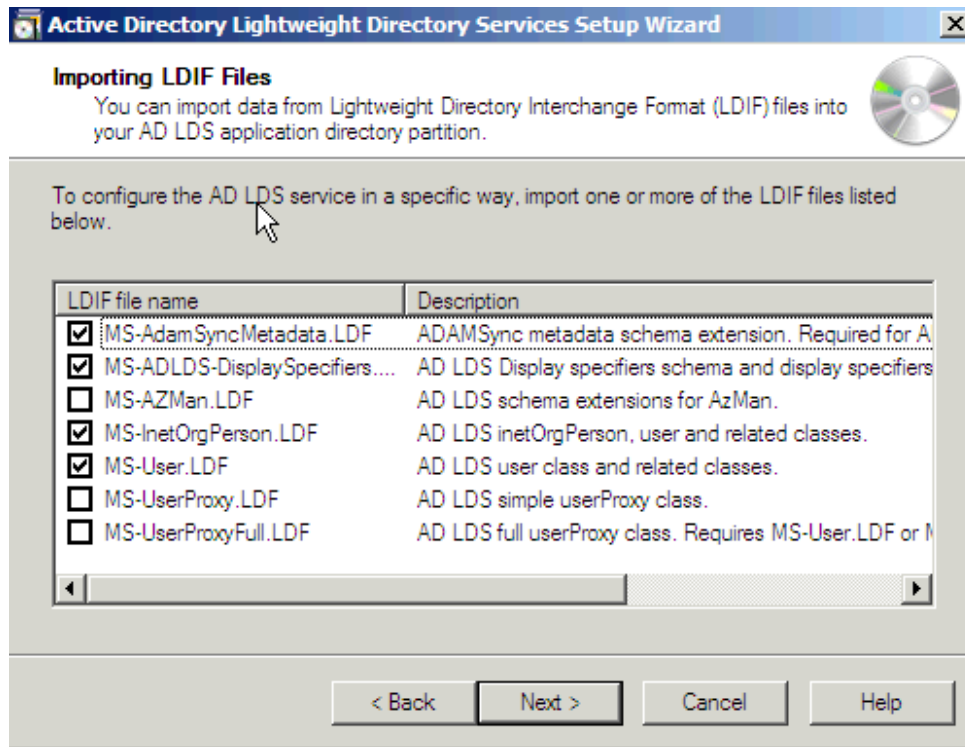


Figure 23: Importing LDIF Files

Note: If ADAM is being installed on a Windows 2003 server, the above screen shows only four options: MS-AZMan.LDF, MS-InetOrgPerson.LDF, MS-User.LDF, and MS-UserProxy.LDF. From these four, select only MS-User.LDF and MS-InetOrgPerson.LDF



Copy the schema from each domain to ADAM

The following process needs to be repeated for each domain for which you need to synchronize. This example only shows the process against one of the domains in the scenario.

1. Open AD DS/LDS schema analyzer (ADSchemaAnalyzer.exe) in the directory c:\windows\adam.
2. Choose File > Load target schema.

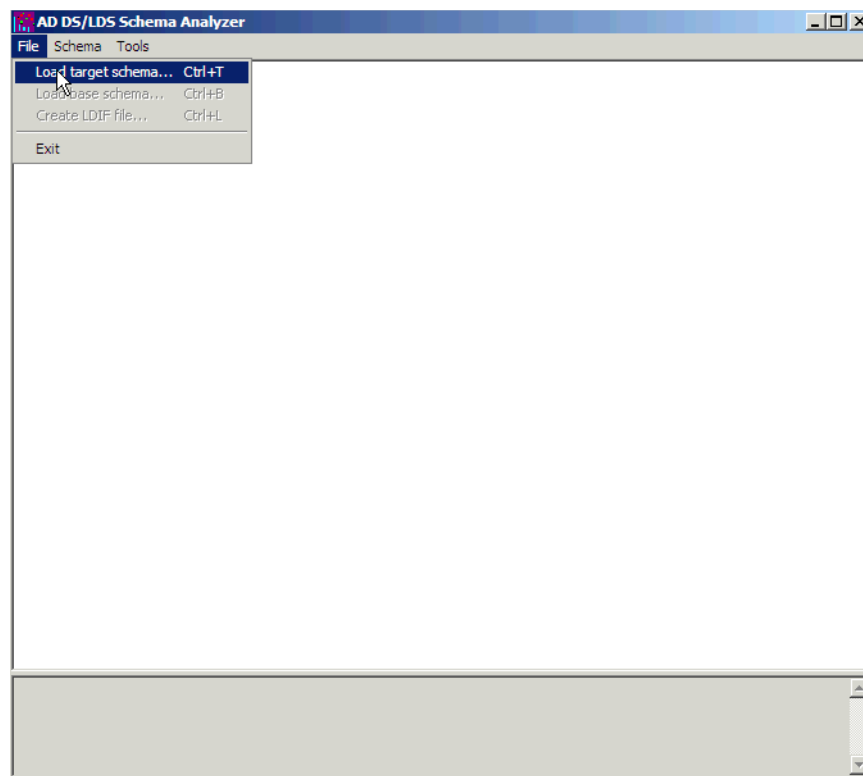


Figure 24: AD DS/LDS Schema Analyzer



3. Provide the credentials of the source AD Domain Controller from which you want to import.

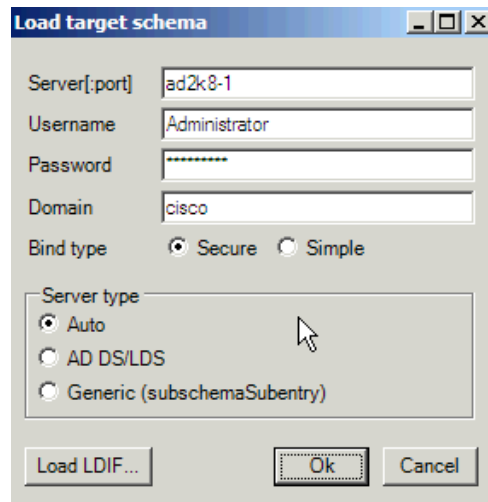


Figure 25: Load target schema

4. Choose File > Load base schema.

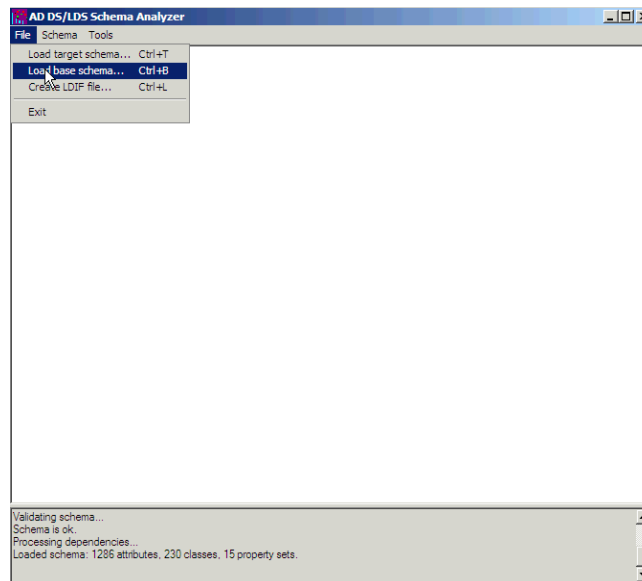


Figure 26: File > Load base schema



5. Specify the AD LDS to which you want to connect and extend the schema.

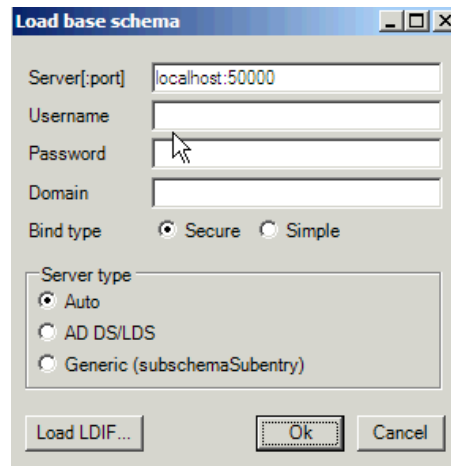


Figure 27: Load base schema

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

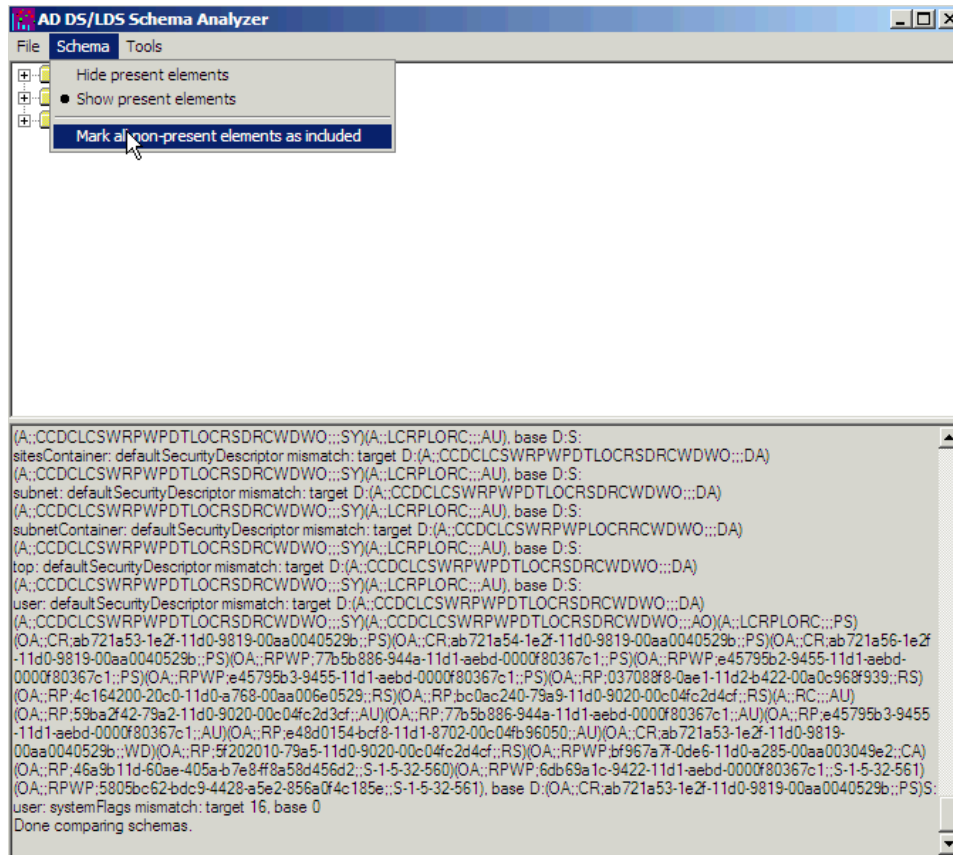


Figure 28: Mark all non-present elements as included



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

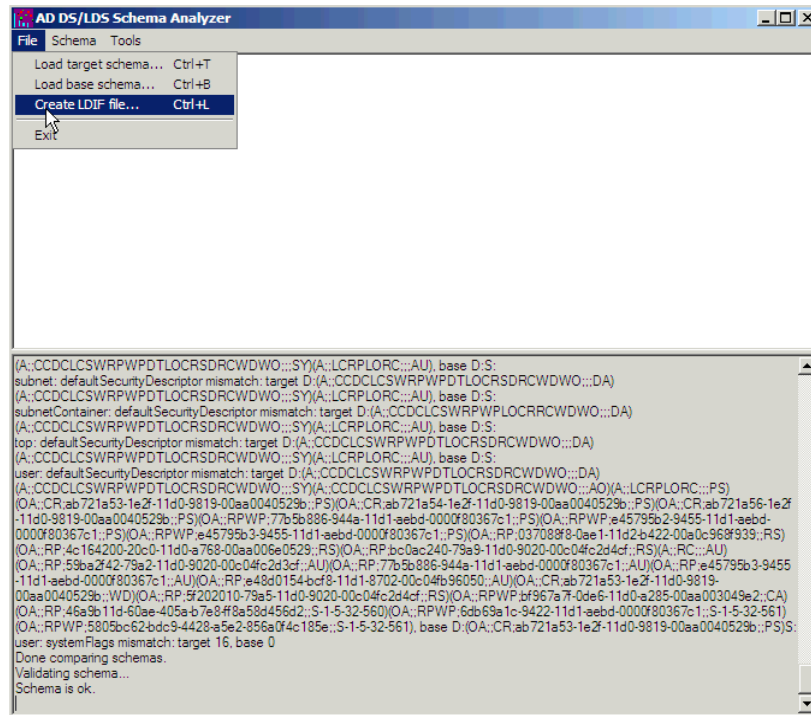


Figure 29: Create LDIF file

One option to help organize the files that need to be generated could be to create a separate directory. This directory will allow the files to be separated from the main c:\windows\adam directory.

8. Open a command prompt and create a log directory in the c:\windows\adam directory.

```
cd \windows\adam
mkdir logs
```

9. Import the ldif schema, created using ADSchemaAnalyzer, 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 Microsoft documentation at the following URL for additional ldifde options and command formats:

<http://support.microsoft.com/kb/237677>



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' is not used. The object class being created, userProxy, allows the bind redirection. The object class detail needs to be created in an 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, using a text edit program, so that it has the following 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
IDAPDisplayName: 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
```

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

1. Save MS-UserProxy-Cisco.ldf file in the C:\windows\adam directory.
2. 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
```

```
Administrator: C:\Windows\system32\cmd.exe
C:\Windows\ADAM>ldifde -i -s localhost:50000 -c CN=Configuration,DC=X #ConfigurationNamingContext -f MS-UserProxy-Cisco.ldf -j c:\windows\adam\logs
Connecting to "localhost:50000"
Logging in as current user using SSPI
Importing directory from file "MS-UserProxy-Cisco.ldf"
Loading entries...
2 entries modified successfully.

The command has completed successfully
C:\Windows\ADAM>_
```

3. If ADAM is being installed on a Windows 2003 server, run the following command as well :

```
C:\WINDOWS\adam>ldifde -i -s localhost:50000 -c CN=Configuration,DC=X #ConfigurationNamingContext -f MS-AdamSyncMetaData.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.

Note: *This step needs to be repeated for each domain that needs to synchronize. This example only shows the process against one of the domains.*

1. Starting with the original MS-AdamSyncConf.xml, 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 the following 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;(objectClass=user)(objectCategory=person))(&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>
        <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>
    </schedule>
  </configuration>
</doc>
```

Cisco Public

Copyright © 2010 Cisco Systems, Inc. All rights reserved.

Page 29 of 44



```
</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>
```

2. In this file, the following 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. 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 (for example, Finance OU), it should be something like `OU=Finance,DC=Cisco,DC=com`.

3. Save the newly created XML file in the `C:\windows\adam` directory.
4. Open a command window: `cd \windows\adam`
5. Run the following command:

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

Notice that the file `AdamSyncConf1.xml` is the newly created XML file.

6. Synchronize the users with the following command:

```
ADAMSync /sync localhost:50000 "dc=cisco,dc=com" /log c:\windows\adam\logs\sync.log
```

The result should be something similar to the following:



```
Administrator: C:\Windows\system32\cmd.exe
Previous entry took 0 seconds <31, 0> to process
Updating the configuration file DirSync cookie with a new value.
Beginning processing of deferred dn references.
Finished processing of deferred dn references.

Finished (successful) synchronization run.
Number of entries processed via dirSync: 10
Number of entries processed via ldap: 0
Processing took 0 seconds <0, 1080778752>.
Number of object additions: 10
Number of object modifications: 0
Number of object deletions: 0
Number of object renames: 0
Number of references processed / dropped: 0, 0
Maximum number of attributes seen on a single object: 10
Maximum number of values retrieved via range syntax: 0

Beginning aging run.
Aging requested every 0 runs. We last aged 1 runs ago.
Saving Configuration File on DC=cisco,DC=com
Saved configuration file.
C:\Windows\ADAM>
```

Figure 31: User Synchronization Results

7. To perform automatic sync from AD to ADAM , use Task scheduler in Windows.
8. Create a bat file with the following content:

"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
9. Schedule the task to run the bat file as required. This ensures that additions, modifications, and deletions in AD get reflected in ADAM as well.
10. We can create another bat file and schedule it to perform automatic sync from the other forest.



Creating the user in AD LDS for Unified CM synchronization and authentication

1. From the Administrator tools in the startup menu, open ADSI Edit.
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).

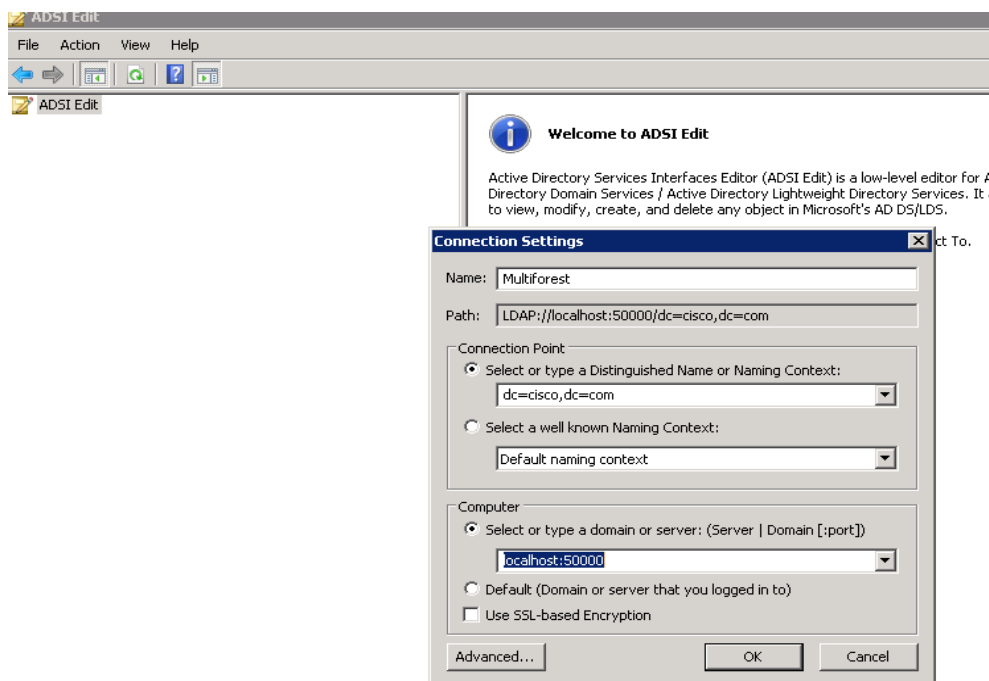


Figure 32: Connection Settings



4. Right-click on the base DN, select New, and select Object.

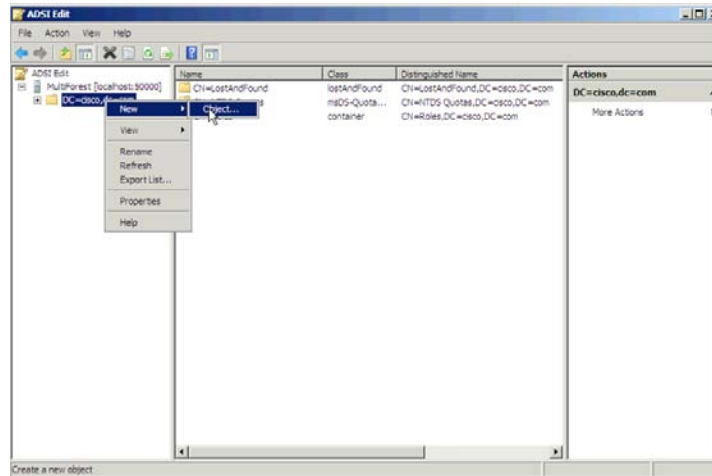


Figure 33: Creating New Object

5. Select a class of user.

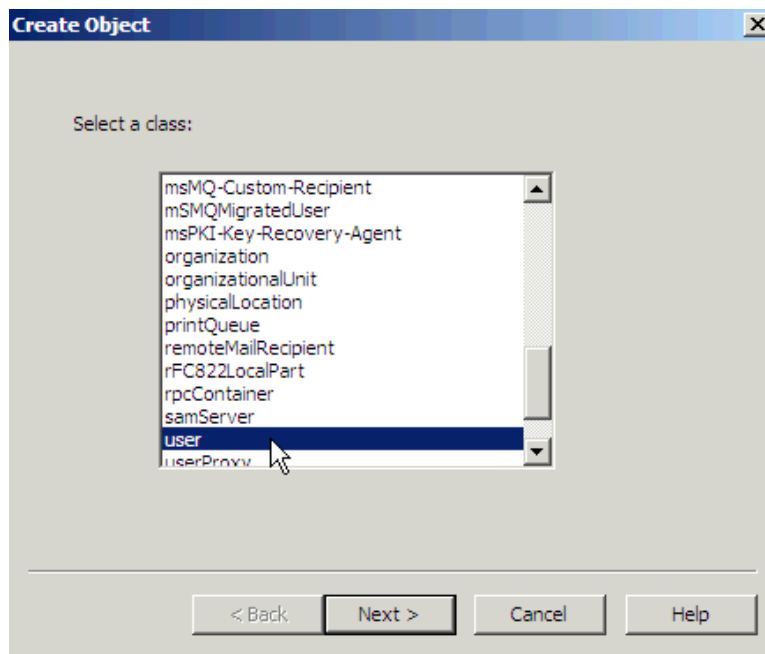


Figure 34: Selecting New User Class



- In this example, “root” was chosen. (Any name can be chosen here.)

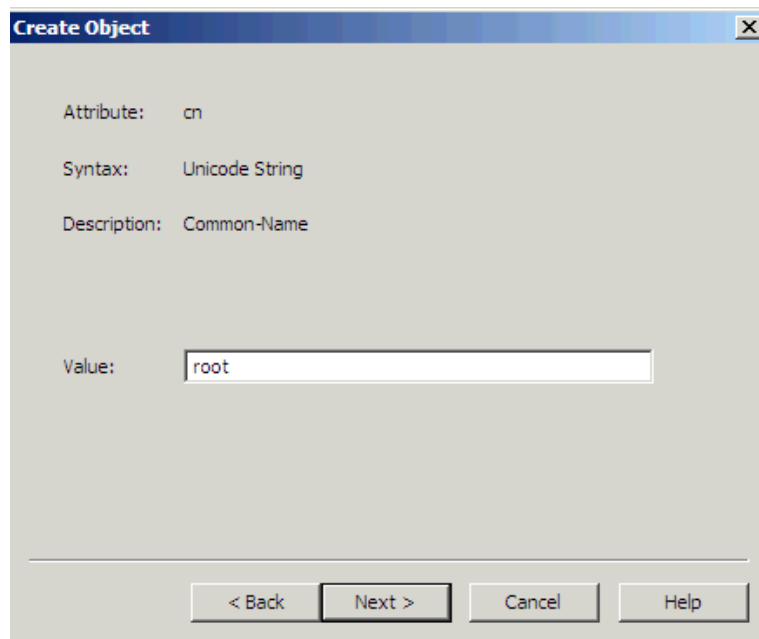


Figure 35: Naming an Object Attribute

- Provide a password to the new user, right-click on the user, and choose Reset Password.

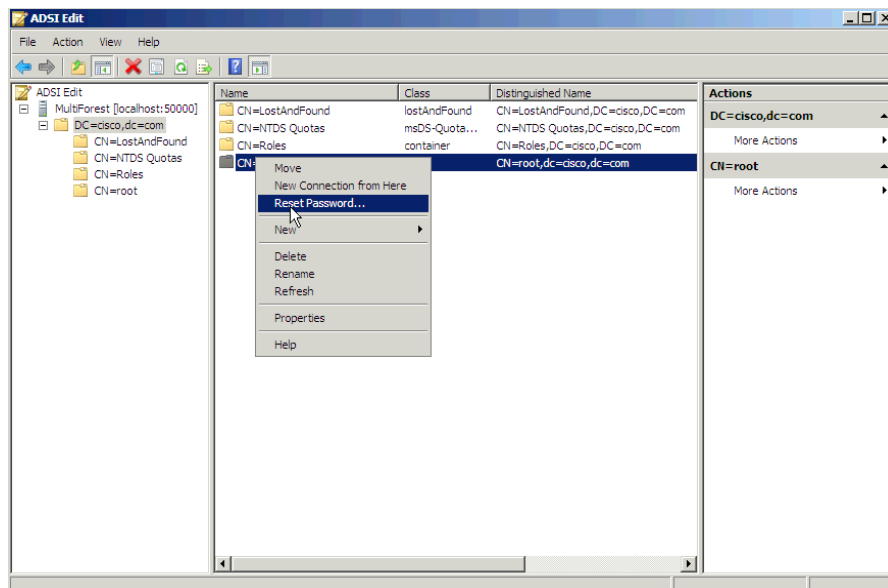


Figure 36: Resetting New User Password



8. Enable the new user, which is disabled by default. Right-click on the user and choose Properties.

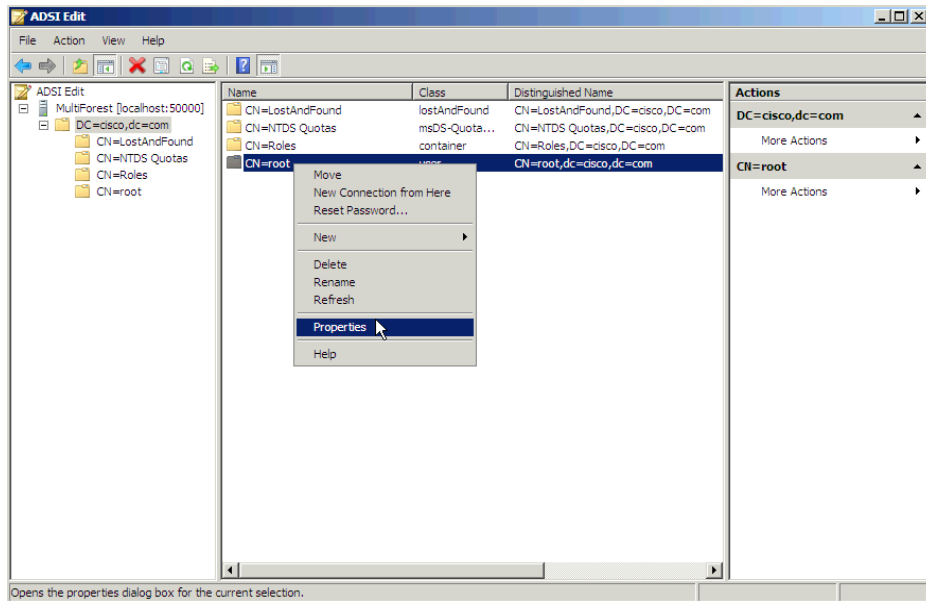


Figure 37: Enabling New User

9. Browse to the msDS-UserAccountDisabled attribute.

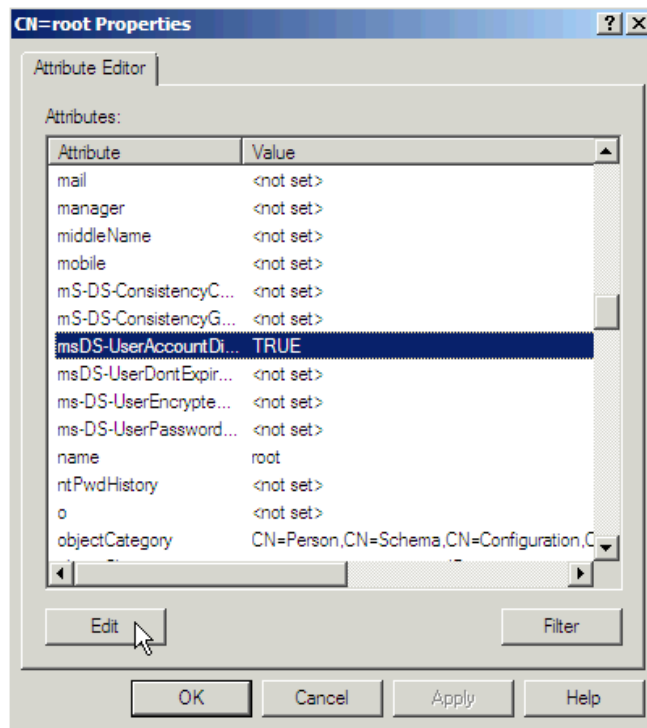


Figure 38: Attribute Editor for User Account

10. Select Edit and change the value to False.

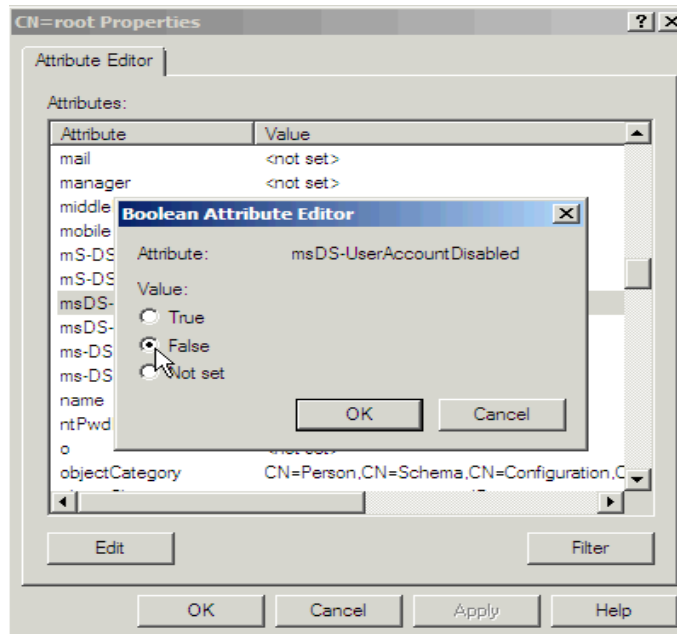


Figure 39: Boolean Attribute Editor

11. The new user needs to be added to one group that has reading permission to the AD LDS. In this example, Administrators was chosen.
12. Browse to the “CN=Roles,CN=Administrators” container, right-click on it, and choose Properties.

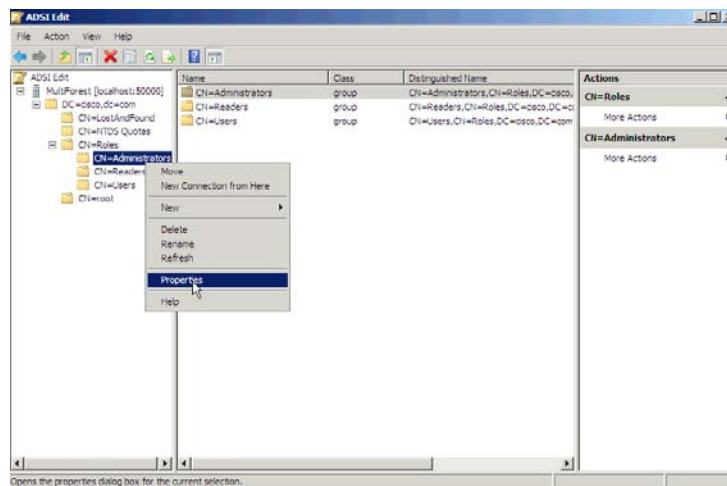


Figure 40: Properties of CN=Administrators



13. Browse to the *member* attribute, and edit it.

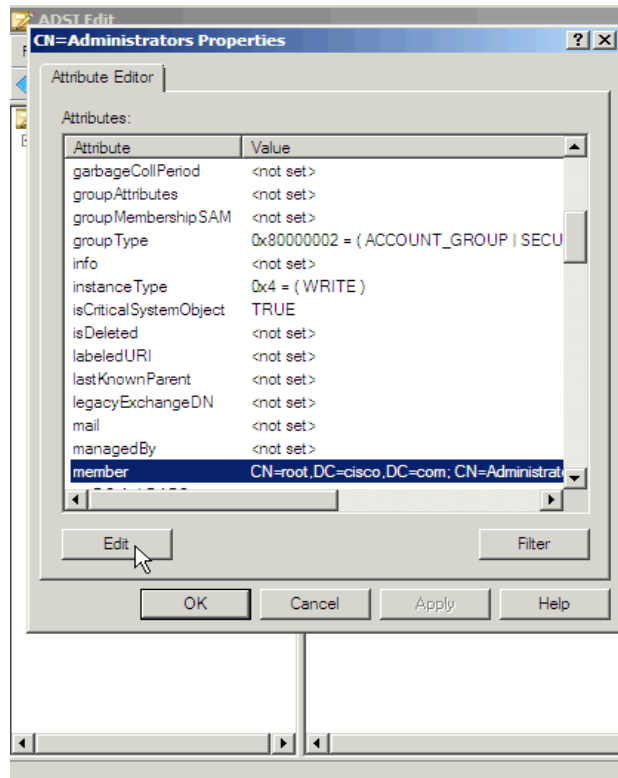


Figure 41: Attribute Editor for member Attribute

14. Add the new Distinguished Name (DN) that was previously created, `cn=root,dc=Cisco,dc=com`, to this group.

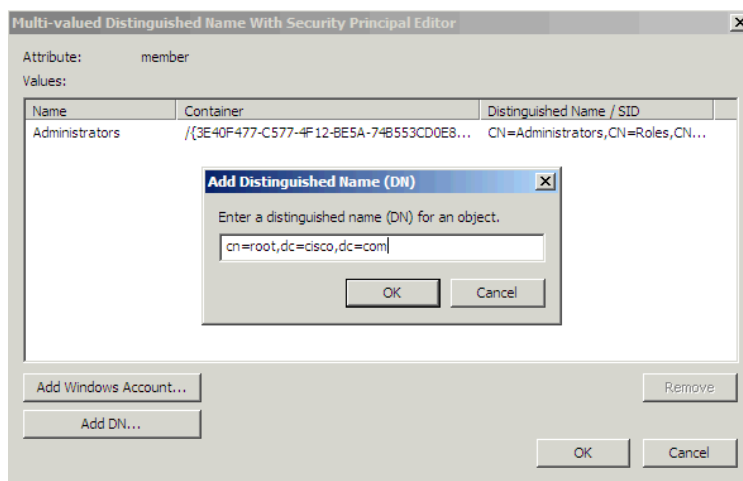


Figure 42: Add Distinguished Name



15. Update the schema and restart AD LDS.

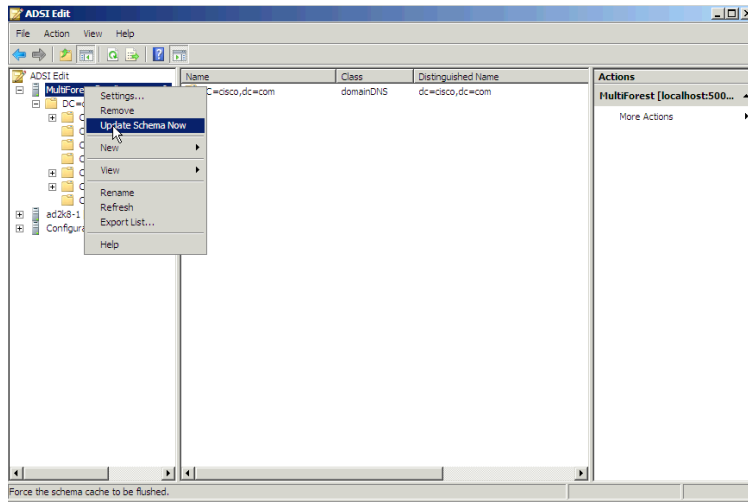


Figure 43: Update Schema Now

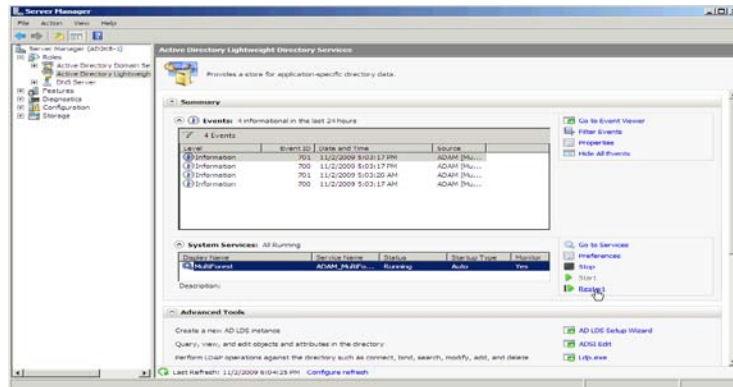


Figure 44: Restarting AD LDS



Configuring 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 is running 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.

Note

Disabling the requirement for SSL for bind redirection causes the password of a Windows security principal to pass to the computer that is running ADAM without encryption. Thus, you should only disable the SSL requirement in a test environment.

By default SSL is enabled, complete the following steps:

1. Generate the certificate for ADAM/AD LDS. Consult Microsoft documentation for information regarding ADAM/AD LDS certification generation.
2. Upload the ADAM/AD LDS certificate to Unified CM. Refer to the Cisco Unified Communications Operations System Administration Guide for additional details http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html
3. Select the checkbox to use SSL in LDAP Directory page and LDAP Authentication page.
4. Give 50001 (in our example) for LDAP port, which is the SSL port number given while installing ADAM/AD LDS instance.

To disable the SSL requirement for bind redirection

1. Click **Start**, point to **Administrative Tools**, and then click **ADSI Edit**.
2. On the **Action** menu, click **Connect to**.
3. In **Select or type a domain or server: (Server | Domain[:port])**, type **localhost:50000** (This is the ADAM host and port.)
4. Under **Connection point**, click **Select a well-known naming context**, click **Configuration**, and then click **OK**.
5. In the console tree, browse to the following container object in the configuration partition: **CN=Directory Service,CN=Windows NT,CN=Services**.
6. Right-click **CN=Directory Service**, and then click **Properties**.
7. In **Attributes**, click **msDS-Other-Settings**, and then click **Edit**.
8. In **Values**, click **RequireSecureProxyBind=1**, and then click **Remove**.
9. In **Value to add**, type **RequireSecureProxyBind=0**, click **Add**, and then click **OK**.
10. Restart AD LDS for the changes to take effect.

You can get more information at the following URL:

<http://technet.microsoft.com/en-us/library/cc784622%28WS.10%29.aspx>



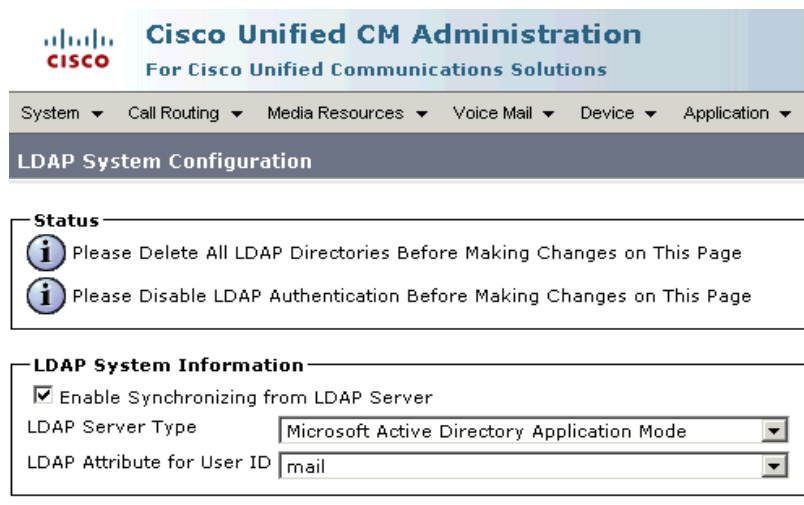
Configuring Unified CM

ADAM/AD LDS synchronization and authentication is supported in Unified CM version 8.0(1) and later.

1. Choose System > LDAP > LDAP System.

To map the Cisco UserID to mail, employeeNumber, or telephoneNumber:

- A. Select Microsoft Active Directory Application Mode.
- B. Select from any of the following LDAPuserid attributes: mail, employeeNumber or telephoneNumber.



The screenshot shows the Cisco Unified CM Administration interface for LDAP System Configuration. At the top, there is a navigation bar with the Cisco logo and the text "Cisco Unified CM Administration For Cisco Unified Communications Solutions". Below this is a breadcrumb trail: System > Call Routing > Media Resources > Voice Mail > Device > Application. The main heading is "LDAP System Configuration".

Status

- i** Please Delete All LDAP Directories Before Making Changes on This Page
- i** Please Disable LDAP Authentication Before Making Changes on This Page

LDAP System Information

- Enable Synchronizing from LDAP Server
- LDAP Server Type: Microsoft Active Directory Application Mode
- LDAP Attribute for User ID: mail

Figure 45: LDAP System Configuration



To map the Cisco UserID to *samAccountName* as the LDAP userid attribute:

- A. Select Microsoft Active Directory (rather than Microsoft Active Directory Application Mode)
- B. Select *sAMAccountName* from the LDAP userid attribute drop-down menu.

System ▾ Call Routing ▾ Media Resources ▾ Voice Mail ▾ Device ▾ Application ▾ U

LDAP System Configuration

Save

Status

Status: Ready

LDAP System Information

Enable Synchronizing from LDAP Server

LDAP Server Type

LDAP Attribute for User ID

Figure 46: LDAP System Configuration



2. Configure LDAP synchronization with the credentials of the user that was created in AD LDS. If SSL is desired and the steps to use SSL have been completed, specify the appropriate port (e.g. 50001) and check “Use SSL”

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾

LDAP Directory Related Links: [Back to LDAP Directory Find/L](#)

LDAP Directory Information

LDAP Configuration Name*

LDAP Manager Distinguished Name*

LDAP Password*

Confirm Password*

LDAP User Search Base*

LDAP Custom Filter

LDAP Directory Synchronization Schedule

Perform Sync Just Once

Perform a Re-sync Every* DAY ▾

Next Re-sync Time (YYYY-MM-DD hh:mm)*

User Fields To Be Synchronized

| Cisco Unified Communications Manager User Fields | LDAP User Fields | Cisco Unified Communications Manager User Fields | LDAP User Fields |
|--|--|--|-----------------------------------|
| User ID | mail | First Name | givenName |
| Middle Name | <input type="text" value="middleName"/> | Last Name | sn |
| Manager ID | manager | Department | department |
| Phone Number | <input type="text" value="telephoneNumber"/> | Mail ID | <input type="text" value="mail"/> |

LDAP Server Information

Host Name or IP Address for Server* LDAP Port* Use SSL

Figure 47: LDAP Directory



1. Configure LDAP authentication with the credentials of the user that was created in AD LDS. If SSL is desired and the steps to use SSL have been completed, specify the appropriate port (e.g. 50001) and check “Use SSL”

The screenshot shows the Cisco Unified CM Administration interface for LDAP Authentication. The page title is "Cisco Unified CM Administration For Cisco Unified Communications Solutions". The navigation menu includes System, Call Routing, Media Resources, Voice Mail, Device, Application, User Management, and Bulk Ad. The main content area is titled "LDAP Authentication" and contains a "Save" button. Below this is a "Status" section showing "Status: Ready". The "LDAP Authentication for End Users" section has a checked box for "Use LDAP Authentication for End Users" and four input fields: "LDAP Manager Distinguished Name*" (cn=root,dc=cisco,dc=com), "LDAP Password*" (masked with dots), "Confirm Password*" (masked with dots), and "LDAP User Search Base*" (dc=cisco,dc=com). The "LDAP Server Information" section has a table with columns "Host Name or IP Address for Server*", "LDAP Port*", and "Use SSL". The first row contains "172.18.36.240", "50000", and an unchecked checkbox. Below the table is a button "Add Another Redundant LDAP Server". At the bottom of the form is another "Save" button.

Figure 48: LDAP Authentication

After the users from AD LDS have been synchronized into Unified CM, the users must be configured and assigned to the ‘Standard CCM Users’ group. Any attempt with LDAP Authentication will fail if the users are not assigned to the user group.



Creating a Custom LDAP filter in Unified CM

The object class, User, is no longer being used; therefore, the ldap filter needs to be changed to use userProxy instead of User.

The default filter must be changed.

Default Filter

```
(&(objectclass=user)(!(objectclass=Computer))(!(ms DS-UserAccountDisabled=TRUE)))
```

Create the Custom Filter (Required):

```
(&(objectclass=userProxy)(!(objectclass=Computer))(!(ms DS-UserAccountDisabled=TRUE)))
```

To create the custom filter on Unified CM 8.0(1):

1. Log in to Cisco Unified CM Administration using a web browser
2. Select the LDAP Custom Filter option from the LDAP configuration menu.
3. Create a new filter using the example above
4. Save the filter
5. Assign the filter to each applicable Synchronization Agreement

LDAP Filter Configuration

Save

Status

Status: Ready

LDAP Custom Filter Information

Filter Name* CustomFilter

Filter* (&(objectclass=userProxy)(!(objectclass=Computer))

Save

Figure 49: LDAP Filter Configuration

This filter is used in the LDAP directory page while configuring LDAP synchronization agreement as shown in Figure 47.