

Cisco Show and Share in a Multi-Forest Environment

This document discusses using Cisco Show and Share® in a Multi-Forest Environment.

Note: Active Directory Lightweight Directory Services (AD LDS) was known formerly as Active Directory Application Mode (ADAM); these terms are used interchangeably in this document.

Prerequisites

Ensure that you meet these requirements:

- You have knowledge of deploying and configuring Cisco Show and Share and Digital Media Manager (DMM).
- You are responsible for deploying, configuring, and maintaining Microsoft Active Directory Lightweight Directory Services 2008.

Note: The Lightweight Directory Access Protocol (LDAP) authentication user search base must match the ADAM domain as well. If the search base shows "LDAP user search base is formed using the User ID information", you cannot use the attribute that you have selected.

Components Used

The information in this document is based on these software versions:

- Cisco Show and Share Release 5.2.3 or later
- Lightweight Directory Services 2008

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.

Background Information

You can use Microsoft Active Directory Lightweight Directory Services (AD LDS), formerly known as Active Directory Application Mode (ADAM), 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, you can use AD LDS to store the data. You can use AD LDS in conjunction with AD DS, so that you 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 AD replication. You do not have to extend the AD schema to support the application, and you can partition the directory structure so that the AD LDS service is deployed only to the servers that need to support the directory-enabled application.

Many differences exist between ADAM and Active Directory. ADAM can deliver only some of the AD functions, as shown in [Figure 1](#).

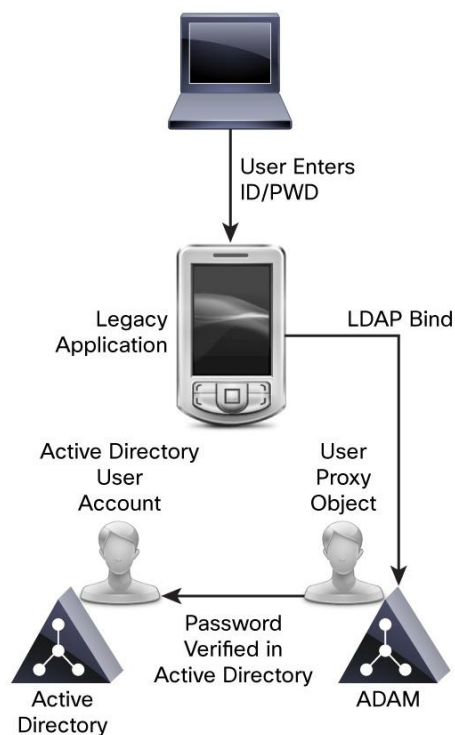
Figure 1. AD and ADAM Functions Comparison

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	

ADAM can create a database of users and store the user details. Single Sign-On (SSO) functions are desired 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, may force you to avoid AD, making ADAM a necessary choice.

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 performing its normal bind operation, the application checks the ID locally but checks the password against Active Directory in the background, as [Figure 2](#) illustrates. The application does not need to be aware of this AD interaction.

Figure 2. ADAM User Proxy Password Authentication



You should use ADAM bind redirection 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 using a special object called a proxy object, an object in ADAM that represents a security principal in AD. Each proxy object in ADAM contains the service identifier (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 plaintext to ADAM because the initial bind request is a simple LDAP bind request. For this reason, a Secure Sockets Layer (SSL) connection is required by default between the directory client and ADAM. ADAM uses Windows Security application programming interfaces (APIs) to present the password to AD.

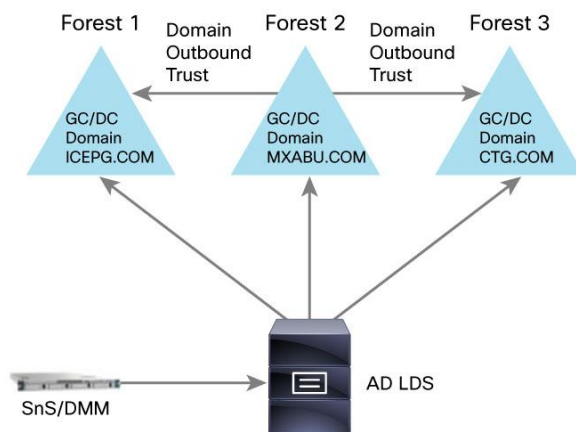
For more information about bind redirection, visit [Understanding ADAM bind redirection](#) on Microsoft.com.

Note: The requirement for SSL when using bind redirection should not be disabled in a production environment.

Active Directory Multiple Forest Support Scenario in Cisco Show and Share

For the purpose of explaining the configuration, we will use an example scenario where company MXABU (Forest 2) has acquired two companies: ICEPG (Forest 1) and CTG (Forest 3). In the migration phase, the AD structure of each company will be integrated, enabling the deployment of a single MXABU cluster ([Figure 3](#)).

Figure 3. Multi-Forest Scenario



In this example, company MXABU (Forest 2) is hosted on a server running Windows 2008 Server Service Pack 2 (SP2). Company ICEPG (Forest 1) has a single domain with a domain controller (DC) that is a Global Catalog hosted on a server running Windows 2008 R2 Server SP2. Company CTG (Forest 3) has a single domain with a DC that is also a Global Catalog hosted on a server running Windows 2008 Server SP2.

AD LDS is installed in the DC for domain MXABU; in fact, you can use any machine anywhere in one of the three forests. However, the Domain Name System (DNS) infrastructure must be in place so that domains in one forest can communicate with domains in other forests and can establish the appropriate trust relationships and validations between the forests.

This section describes the configuration that is required to support the example scenario.

1. Define the Domain Trust Relationship

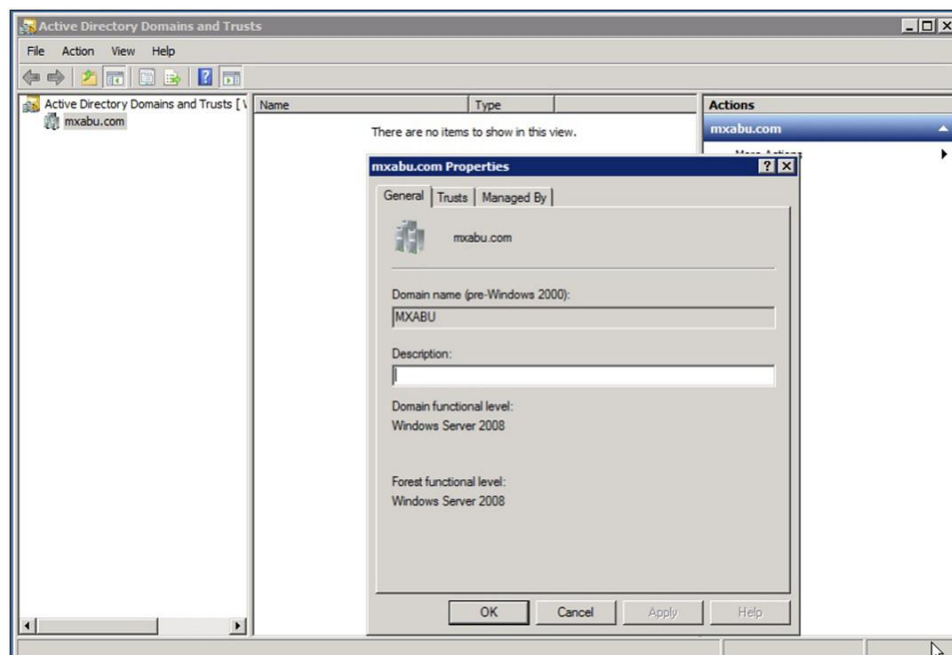
For the authentication of the users to succeed, you need to have a trust between the domain where the ADAM instance is hosted and the other domain(s) that hosts the user accounts. This trust can be a one-way trust if required (outgoing trust from the domain that hosts the ADAM instance to the domain(s)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

Furthermore, you need a user account from both account domains that have 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 DCs.

Perform these steps to set up the inter-trust relationships:

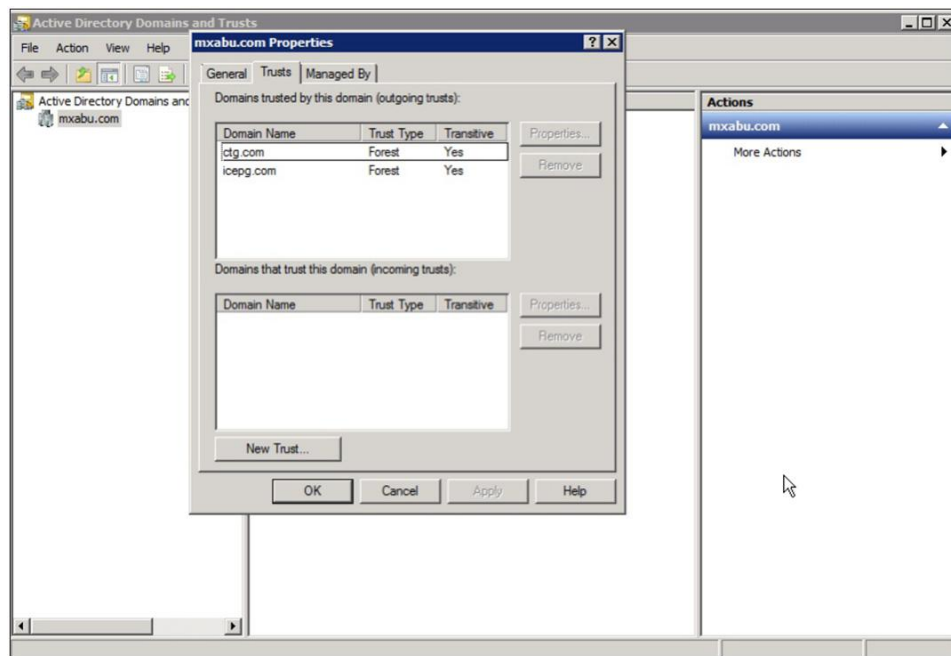
1. Open **Active Directory Domains and Trusts**, choose the domain that hosts AD LDS, right-click on the domain, and choose **Properties**.



Note: We tested the domain functional level and the forest functional level with Lightweight Directory Services 2008.

2. Go to the Trusts tab and click **New Trust**.
3. Follow the wizard and provide the name of the domain with which you want to establish the trust (example: CTG) and click **Next**.
4. In the Trust Type window, choose **Forest trust** and click **Next**.
5. In the Direction of Trust window, choose **One-way: outgoing** (required) and click **Next**.
6. In the Sides of Trust window, allow the wizard to configure both domains. To do so, choose **Both this domain and the specified domain** and click **Next**.

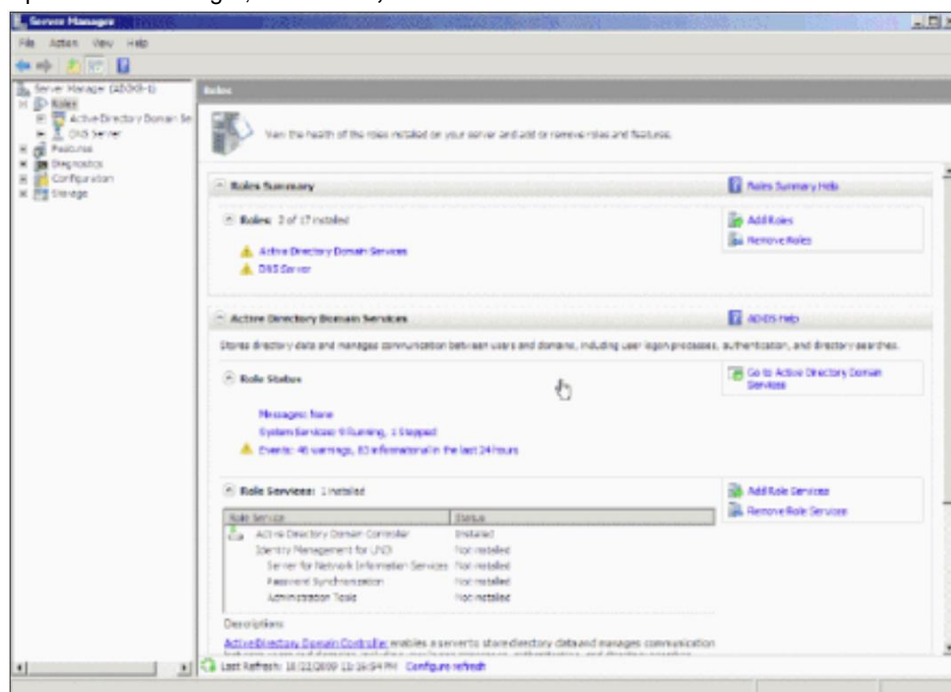
7. In the User Name and Password window, provide the credentials for the other domain. Click **Next**.
8. In the Outgoing Trust Authentication Level - Local Forest window, choose **Forest-wide authentication**. Click **Next**.
9. In the Confirm Outgoing Trust window, choose **Yes, confirm the outgoing trust** and click **Next**. Following is the completed configuration for the example ICEPG and CTG domains:



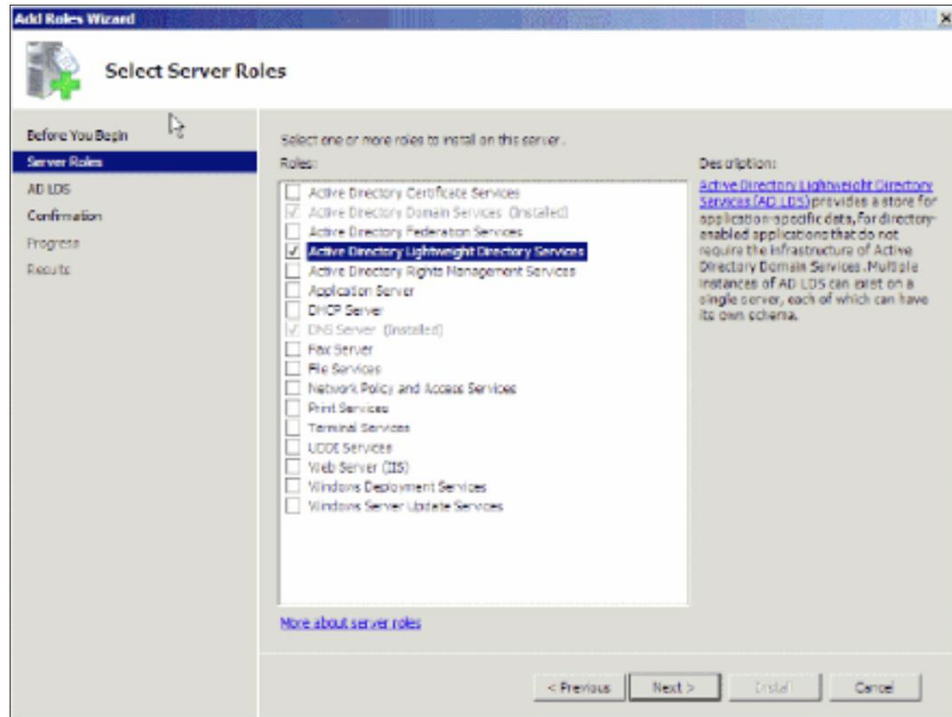
2. Install AD LDS

Perform these steps to install AD LDS:

1. Open Server Manager, click **Roles**, and choose **add New**.



2. In the Select Server Roles window, choose **Active Directory Lightweight Directory Services** and click **Next**. The Installation Progress window displays.



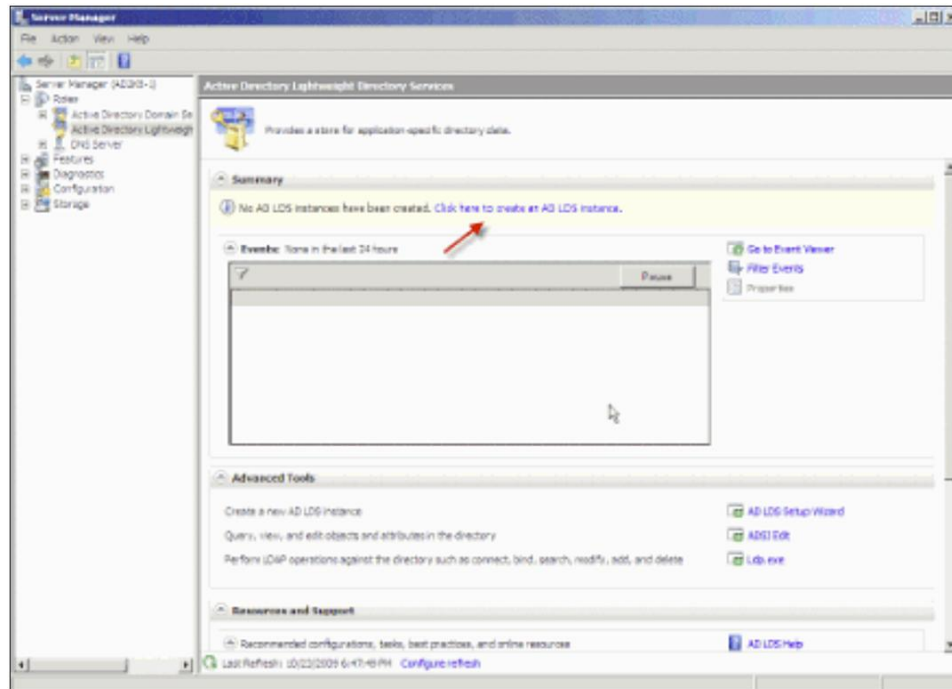
3. Install the Instance for Multiple-Forest Support

AD LDS can run different instances of the services with different ports, enabling different user directory “applications” to run on the same machine. By default, AD LDS chooses ports 389/LDAP and 636/LDAPS. 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.

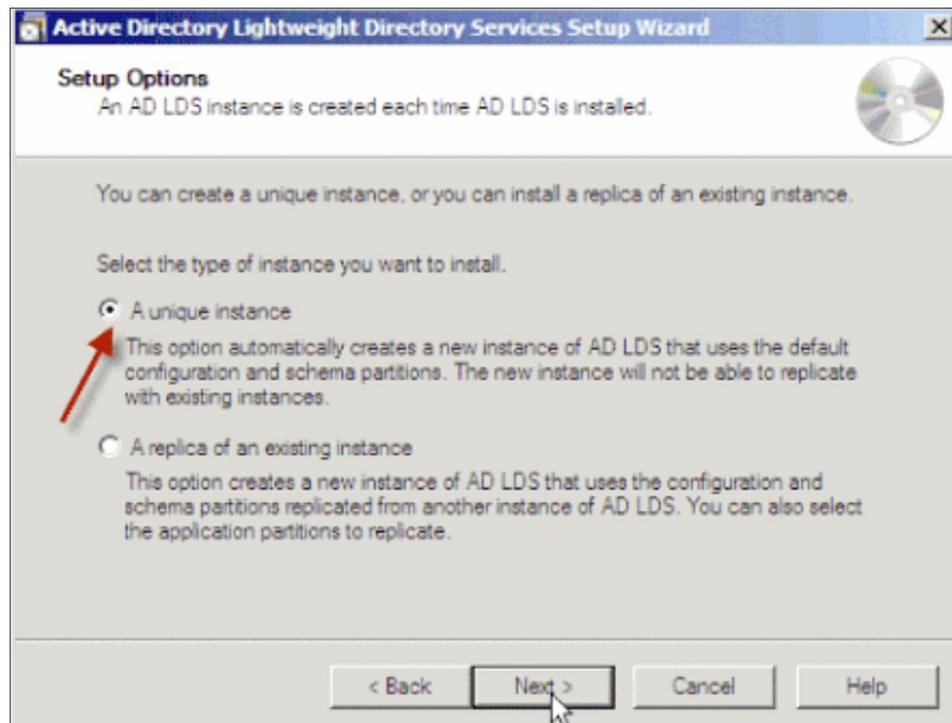
Note: In some cases because of a Microsoft bug, the ports are already in use by the Microsoft DNS server and the instance wizard shows an error, which is not self-explanatory. To resolve this error, reserve the ports in the TCP/IP stack. If you find this problem, refer to [AD LDS service start fails with error "setup could not start the service..." + error code 8007041d](#) on Microsoft.com.

Perform these installation steps:

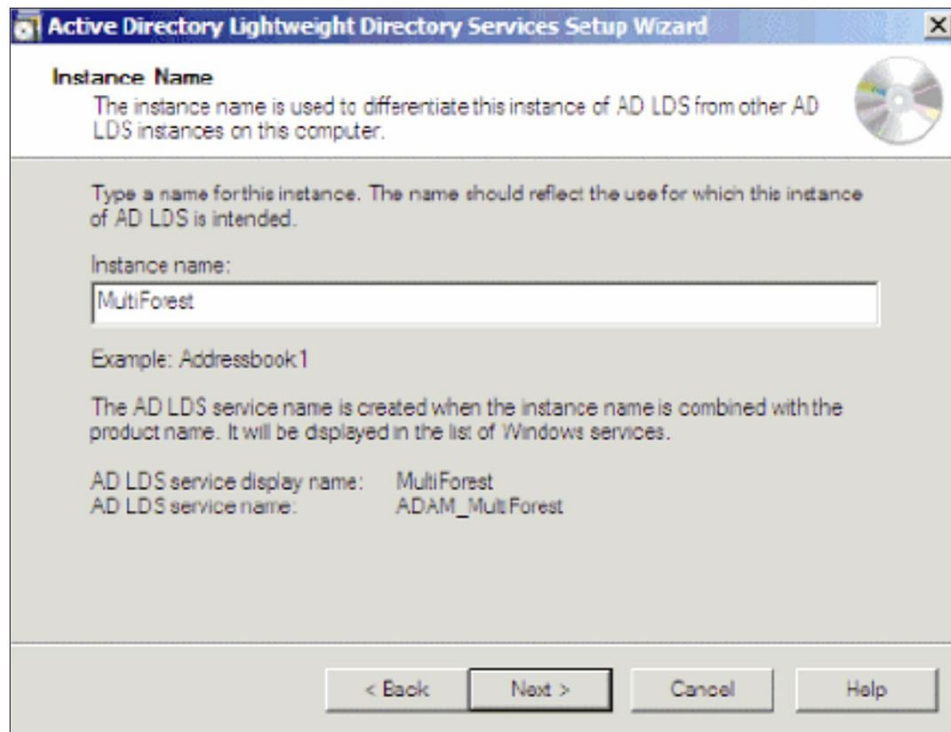
1. In the Server Manager, choose **Roles>AD LDS**.
2. Choose **Click here to create an AD LDS instance**.



3. In the Setup Options window, choose **A unique instance**. Click **Next**.

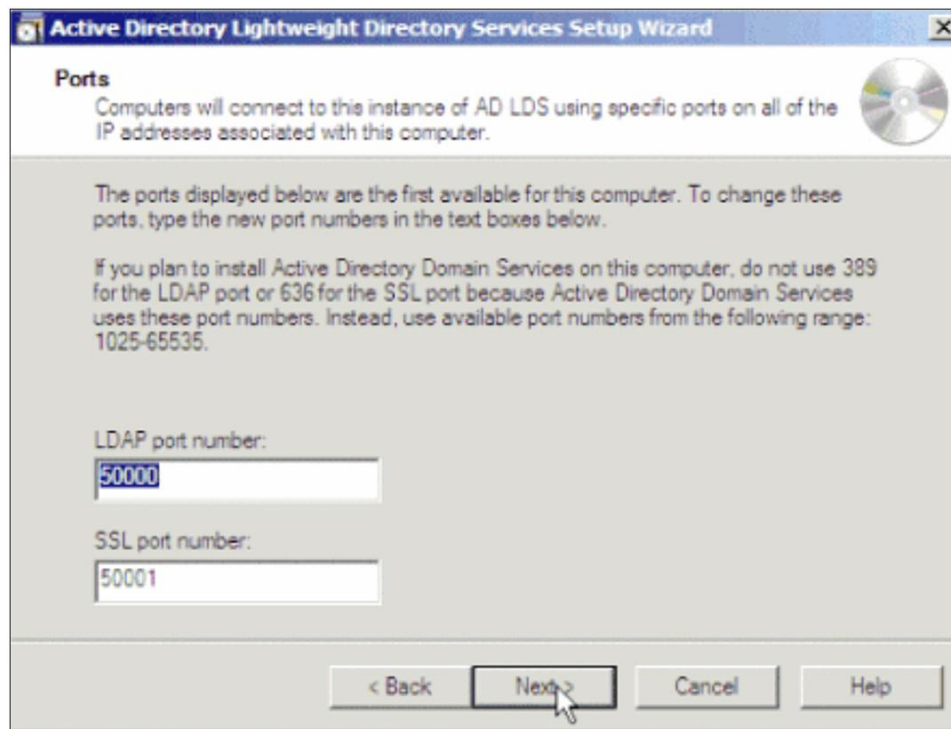


4. In the Instance Name window, provide the name of the instance. In our example, it is MultiForest. Click **Next**.



The screenshot shows the 'Instance Name' window of the 'Active Directory Lightweight Directory Services Setup Wizard'. The window title is 'Active Directory Lightweight Directory Services Setup Wizard'. The main heading is 'Instance Name'. Below it, a text box explains: 'The instance name is used to differentiate this instance of AD LDS from other AD LDS instances on this computer.' To the right of this text is a CD icon. Below the explanation, a text box says: 'Type a name for this instance. The name should reflect the use for which this instance of AD LDS is intended.' Below this is a text input field labeled 'Instance name:' containing the text 'MultiForest'. Below the input field, it says 'Example: Addressbook1'. Further down, it explains: 'The AD LDS service name is created when the instance name is combined with the product name. It will be displayed in the list of Windows services.' Below this, it shows 'AD LDS service display name: MultiForest' and 'AD LDS service name: ADAM_MultiForest'. At the bottom, there are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'. The 'Next >' button is highlighted with a black border.

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



The screenshot shows the 'Ports' window of the 'Active Directory Lightweight Directory Services Setup Wizard'. The window title is 'Active Directory Lightweight Directory Services Setup Wizard'. The main heading is 'Ports'. Below it, a text box explains: 'Computers will connect to this instance of AD LDS using specific ports on all of the IP addresses associated with this computer.' To the right of this text is a CD icon. Below the explanation, it says: 'The ports displayed below are the first available for this computer. To change these ports, type the new port numbers in the text boxes below.' Below this, it provides a warning: 'If you plan to install Active Directory Domain Services on this computer, do not use 389 for the LDAP port or 636 for the SSL port because Active Directory Domain Services uses these port numbers. Instead, use available port numbers from the following range: 1025-65535.' Below this, there are two text input fields. The first is labeled 'LDAP port number:' and contains the value '50000'. The second is labeled 'SSL port number:' and contains the value '50001'. At the bottom, there are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'. The 'Next >' button is highlighted with a black border and a mouse cursor is pointing at it.

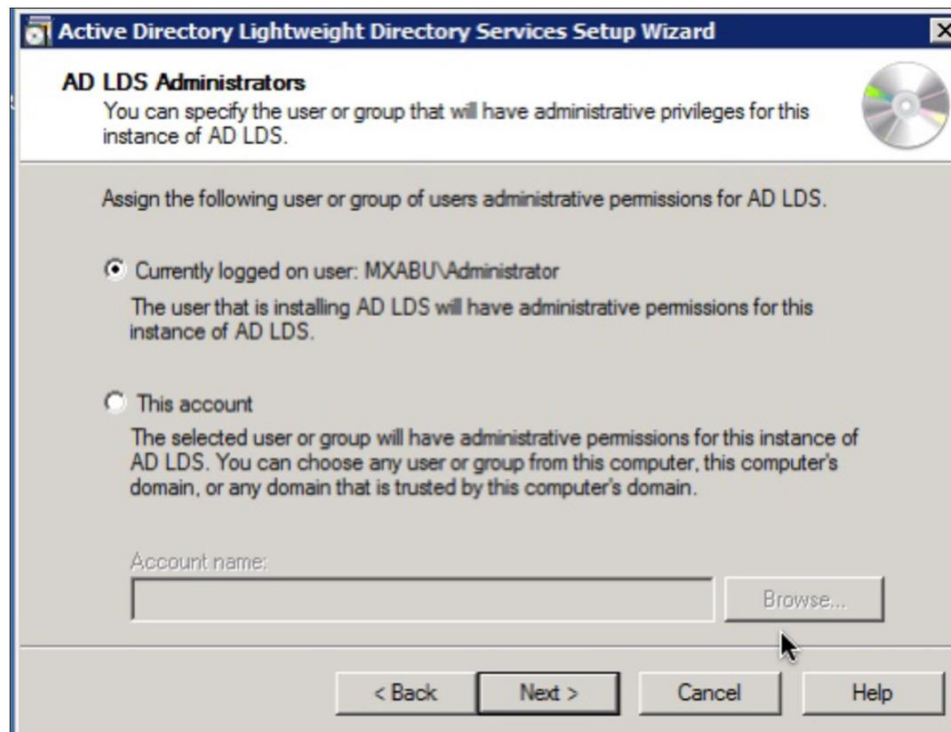
6. In the Application Directory Partition window, provide a partition name for the instance. Do not provide a "CN" such as the one provided in the example of the wizard because most of the time it will create an error in the Schemas. In the example configuration scenario, we chose the same partition as the AD DC that hosts AD LDS (dc=Mxabu,dc=com). Click **Next**.

The screenshot shows the 'Application Directory Partition' window of the 'Active Directory Lightweight Directory Services Setup Wizard'. The window title is 'Active Directory Lightweight Directory Services Setup Wizard'. The main heading is 'Application Directory Partition' with a subtext: 'An application directory partition stores application-specific data.' Below this, a question asks: 'Do you want to create an application directory partition for this instance of AD LDS?'. There are two radio button options: 'No, do not create an application directory partition' and 'Yes, create an application directory partition'. The 'Yes' option is selected. Below the options, a text box labeled 'Partition name:' contains the text 'dc=mxabu,dc=com'. At the bottom, there are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'.

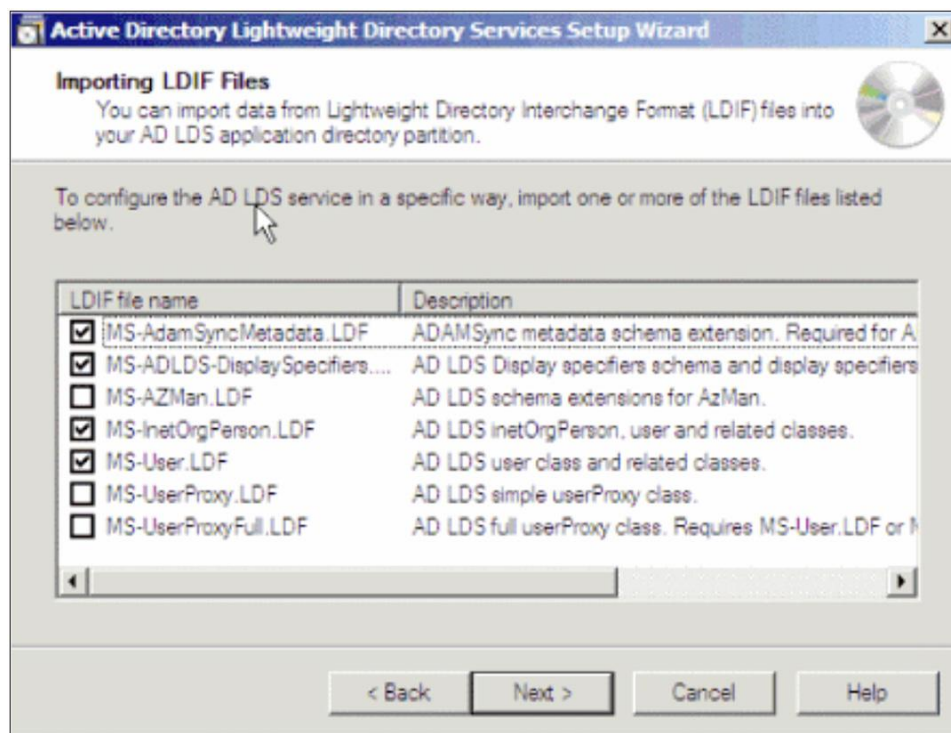
7. In the Service Account Selection window, provide an account to start the server. Click **Next**.

The screenshot shows the 'Service Account Selection' window of the 'Active Directory Lightweight Directory Services Setup Wizard'. The window title is 'Active Directory Lightweight Directory Services Setup Wizard'. The main heading is 'Service Account Selection' with a subtext: 'AD LDS performs operations using the permissions associated with the account you select.' Below this, a text box says: 'Set up AD LDS to perform operations using the permissions associated with the following account.' There are two radio button options: 'Network service account' and 'This account:'. The 'This account:' option is selected. Below the options, there are two text boxes: 'User name:' and 'Password:'. The 'User name:' box contains 'mxabu\Administrator' and has a 'Browse...' button next to it. The 'Password:' box contains a series of dots. At the bottom, there are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'.

8. Provide the name of the user who has administrative permissions. Click **Next**.



9. Import the highlighted default LDAP Data Interchange Format (LDIF) files to build the schema. Click **Next**.

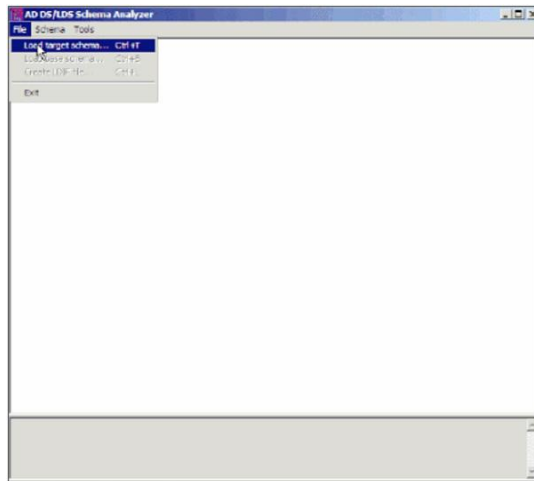


4. Copy the Schema from Each Domain to ADAM

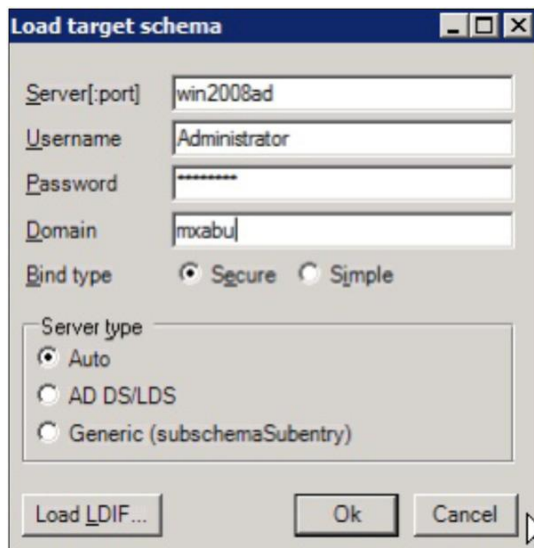
Repeat this process for each domain that you need to synchronize. This example shows only the process against one of the domains in the scenario. If the domains have the same schema, then this process should be done only once.

Perform these steps:

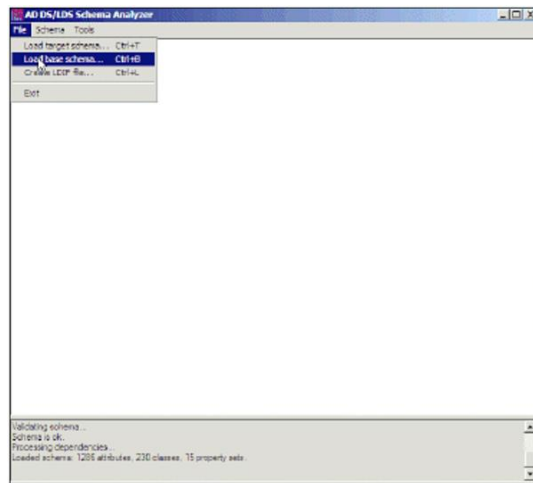
1. Open the AD DS/LDS schema analyzer (**ADSchemaAnalyzer.exe**) in the directory **C:\windows\adam**.
2. Choose **File>Load target schema**.



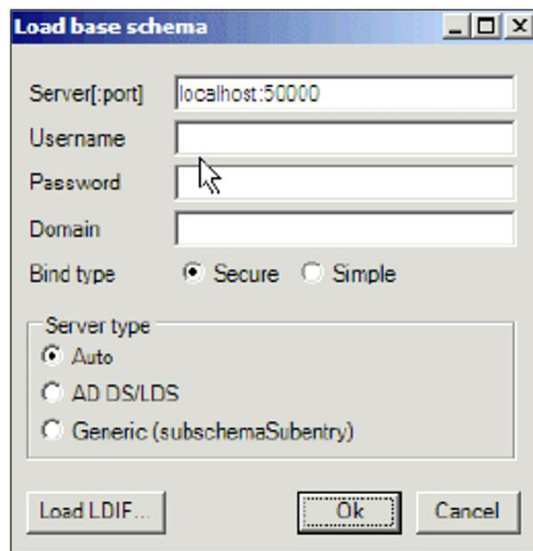
3. Provide the credentials of the source AD DC from which you want to import.



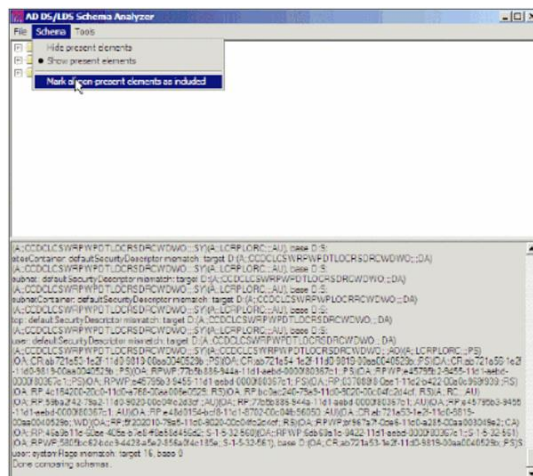
4. Choose **File>Load base schema**.



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

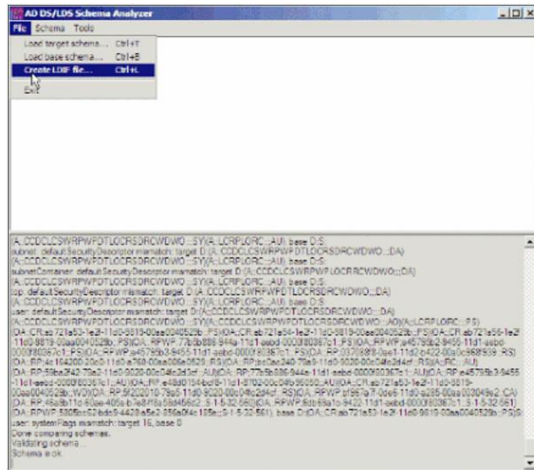


6. Choose **Schema>Mark all non-present elements as included**.



7. Choose **File>Create LDIF file**. In this example, the file created is **diff-schema.ldf**. To simplify the process, create the file in **C:\windows\adam**.

Tip: You can create a separate directory to keep the files that are generated separate from the main **C:\windows\adam** directory.



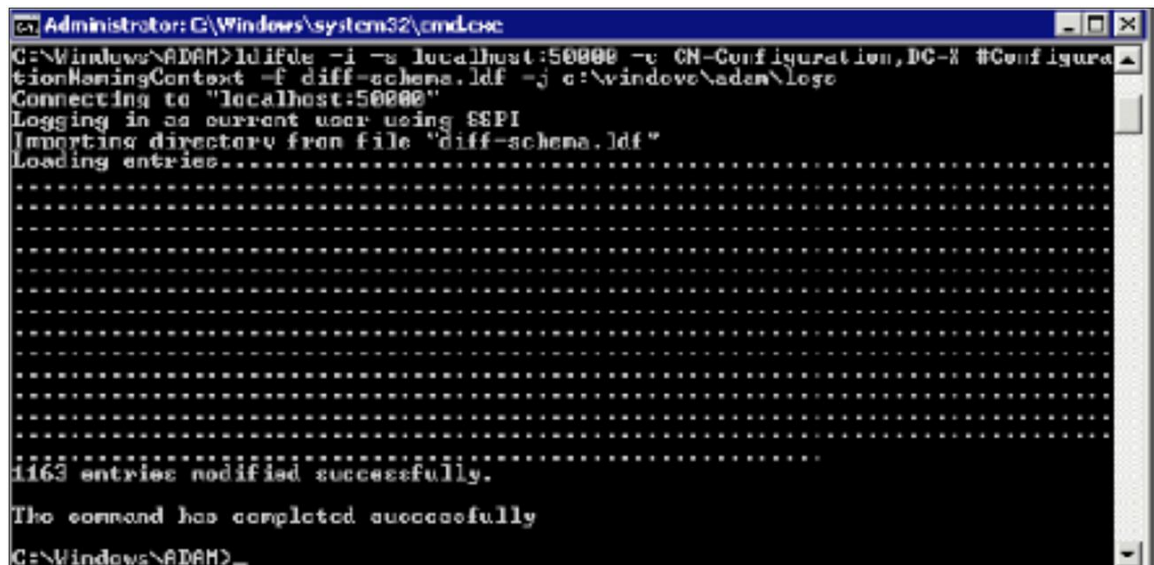
8. Open a command prompt and create a log directory in the **C:\windows\adam** directory:

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

9. Import the LDIF schema that was created using the ADSchemaAnalyzer to AD LDS:

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

For more information about Ldifde options and command formats, go to [Using LDIFDE to import and export directory objects to Active Directory](#) on Microsoft.com.



5. Extend the AD LDS Schema with the User-Proxy Objects

The object for the proxy authentication needs to be created, but do not use the object class **user**. Instead, the object class **userProxy** is created to allow the bind redirection, and the object class detail is created in a new LDIF file. The example file below, **MS-UserProxy-Mxabu.ldf**, was generated from the original MS-UserProxy.ldf and then edited by using a text editor 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-Mxabu.ldf -s localhost:50000 -j
# c:\windows\adam\logs -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

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

Perform these steps:

1. Save the **MS-UserProxy-Mxabu.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-Mxabu.ldf -j c:\windows\adam\logs
```



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

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


6. Import Users from AD DC to AD LDS

The user from each domain now needs to be imported to AD LDS.

Note:

- You must add a service account from each of the domains to the Administrators group in the LDS server.
- Repeat this step for each domain that needs to be synchronized. This example shows the process against only two of the domains.

Perform these steps:

First Domain: **MXABU.COM**

1. Starting with the original MS-AdamSyncConf.xml file, create an XML file for each domain that needs to be synchronized and modify the file with the details specific to each domain so that it has the following content:

```
<?xml version="1.0"?>
<doc>
<configuration>
<description>mxabu.com</description>

<security-mode>object</security-mode>
<source-ad-name>mxabu.com</source-ad-name>
<source-ad-partition>dc=mxabu,dc=com</source-ad-partition>
<source-ad-account></source-ad-account>
<account-domain></account-domain>

<target-dn>dc=mxabu,dc=com</target-dn>
<query>
<base-dn>dc=mxabu,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>
<schtasks-cmd></schtasks-cmd>
</schedule>
</configuration>
<synchronizer-state>
<dirsnc-cookie></dirsnc-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, place the following tags to match the domain:

- **<source-ad-name>**: Use the DNS name of the domain, for example, mxabu.com.
- **<source-ad-partition>**: Use the root partition from the source AD DC that you want to import from; for example, dc=Mxabu, dc=com.
- **<base-dn>**: Choose the container to import from. If all users of the domain are required, this container would be the same as **<source-ad-partition>**, but if users are from a specific organizational unit, for example, Finance OU, it would be similar to OU=Finance,DC=Mxabu,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 AdamSyncConfMxabu.xml/log logs\install.log
```

Note: The file **AdamSyncConfMxabu.xml** is the newly created XML file.

6. Synchronize the users with the following command:

```
ADAMSync/sync localhost:50000 "dc=mxabu,dc=com"/log logs\sync.log
```

The log result should be similar to the following:

```
Adding target object CN=Administrator,CN=Users,dc=mxabu,dc=com.
Adding attributes: sourceobjectguid, instanceType, objectSid, SAMAccountName, lastagedchange, ob
Conflicting object detected. Requesting rename.

Renaming conflicting target object CN=Administrator,CN=Users,dc=mxabu,dc=com to CN=445216f1-9a21
Previous entry took 0 seconds (0, 0) to process

Processing Entry: Page 1, Frame 1, Entry 3, Count 2, USN 0
Processing source entry <guid=475e9fd29c173747af29ed3e62c67228>
Processing in-scope entry 475e9fd29c173747af29ed3e62c67228.
Adding target object CN=Administrator,CN=Users,dc=mxabu,dc=com.
Adding attributes: sourceobjectguid, instanceType, objectSid, SAMAccountName, lastagedchange, ob
Previous entry took 0 seconds (0, 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 dirsSync: 6
Number of entries processed via ldap: 0
Processing took 0 seconds (0, 0).
Number of object additions: 5
Number of object modifications: 1
Number of object deletions: 0
Number of object renames: 1
Number of references processed / dropped: 0, 0
Maximum number of attributes seen on a single object: 6
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=mxabu,DC=com
Saved configuration file.
```

Second Domain: **ICEPG.COM**

1. Starting with the original MS-AdamSyncConf.xml file, create an XML file for each domain that needs to be synchronized and modify the file with the details specific to each domain so that it has the following content:

```
<?xml version="1.0"?>
<doc>
<configuration>
<description>icepg.com</description>

<security-mode>object</security-mode>
<source-ad-name>icepg.com</source-ad-name>
<source-ad-partition>dc=icepg,dc=com</source-ad-partition>
<source-ad-account></source-ad-account>
<account-domain></account-domain>

<target-dn>dc=mxabu,dc=com</target-dn>
<query>
<base-dn>dc=icepg,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>
<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 DNS name of the domain; for example, icepg.com.
 - <source-ad-partition>: Use the root partition from the source AD DC that you want to import from; for example, dc=icepg, dc=com.
 - <base-dn>: Choose the container to import from. If all users of the domain are required, this container would be the same as <source-ad-partition>, but if users are from a specific organizational unit, for example, Finance OU, it would be similar to OU=Finance,DC=icepg,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:

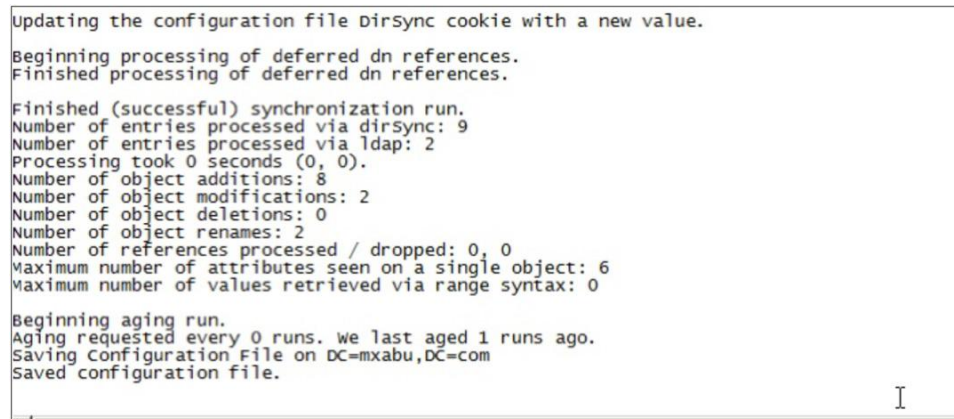
```
ADAMSync/install localhost:50000 AdamSyncConfIcepg.xml/log logs\install.log
```

Note: The file **AdamSyncConfIcepg.xml** is the newly created XML file.

6. Synchronize the users with the following command:

```
ADAMSync/sync localhost:50000 "dc=mxabu,dc=com"/log logs\sync.log
```

The log result should be similar to the following:



```
Updating the configuration file DirsSync 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 dirsSync: 9
Number of entries processed via ldap: 2
Processing took 0 seconds (0, 0).
Number of object additions: 8
Number of object modifications: 2
Number of object deletions: 0
Number of object renames: 2
Number of references processed / dropped: 0, 0
Maximum number of attributes seen on a single object: 6
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=mxabu,DC=com
Saved configuration file.
```

7. To perform a periodic sync from AD to ADAM, use the Task Scheduler in Windows.

8. Create a .cmd or .bat file with the following content:

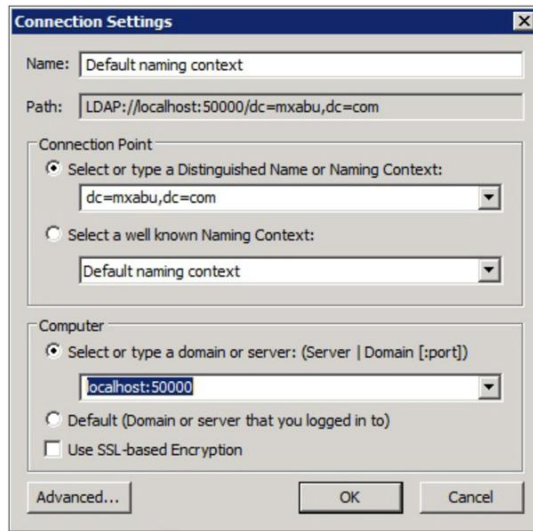
```
cd \Windows\ADAM
ADAMSync /install localhost:50000 AdamSyncConfMxabu.xml /log logs\install.log
ADAMSync /sync localhost:50000 "dc=mxabu,dc=com" /log logs\sync.log
ADAMSync /install localhost:50000 AdamSyncConfIcepg.xml /log logs\install.log
ADAMSync /sync localhost:50000 "dc=mxabu,dc=com" /log logs\sync.log
```

9. Schedule the task to run the .cmd or .bat file as required. This process helps ensure that additions, modifications, and deletions in AD are reflected in ADAM.
10. You can create another .cmd or .bat file and schedule it to perform a periodic sync from the other forest.

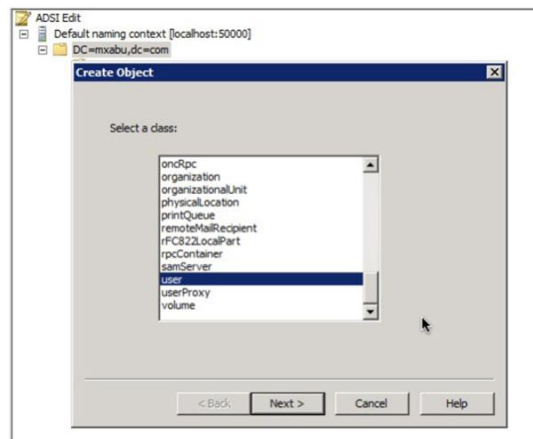
7. Create the User in AD LDS for DMM Synchronization and Cisco Show and Share Authentication

Perform these steps:

1. From the Administrator tools in the Start menu, open **ADSI Edit**.
2. On the Action menu, choose **Connect to**.
3. Connect to base DN of the AD LDS tree (DC=Mxabu,DC=com) and specify the host and port where it is hosted (localhost:50000). Click **OK**.

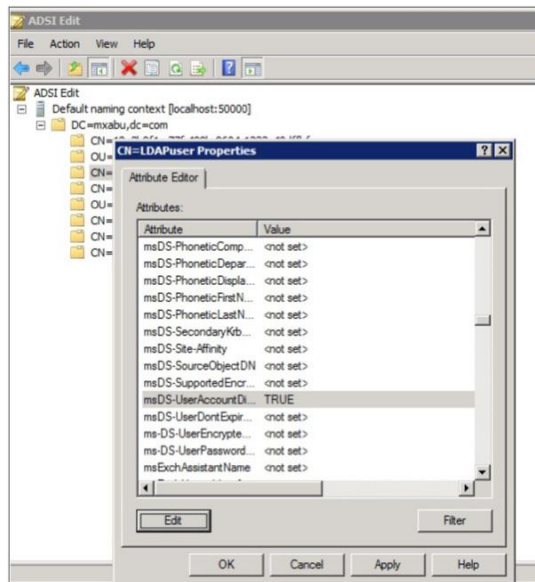


4. Right-click on the base DN, and then choose **New>Object**.

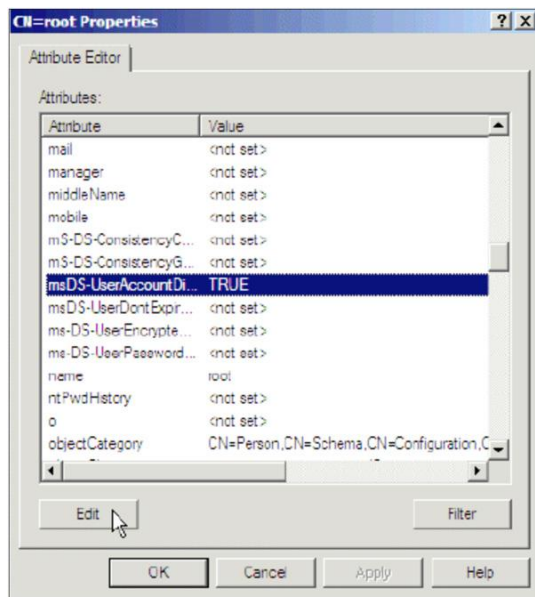


5. Select a class of user and click **Next**. In this example, "LDAPuser" was chosen, but you can choose any name here.
6. Provide a password for the new user, right-click on the user, and then choose **Reset Password**.

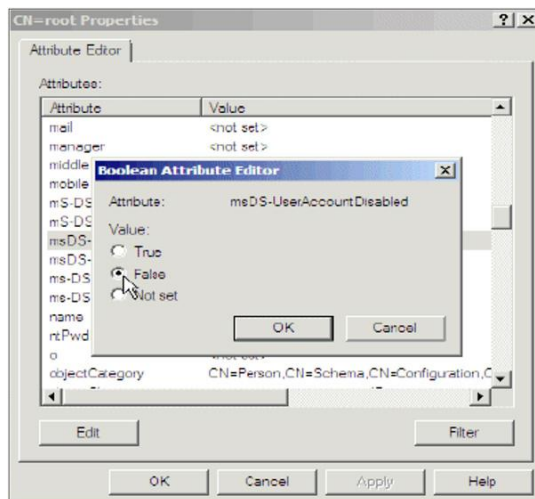
7. Enable the new user; it is disabled by default. Right-click on the user and choose **Properties**.



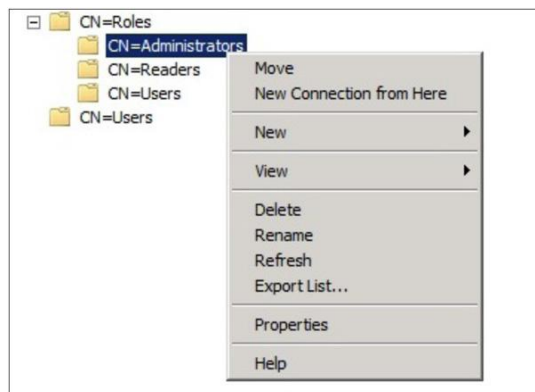
8. Browse to the **msDS-UserAccountDisabled** attribute.



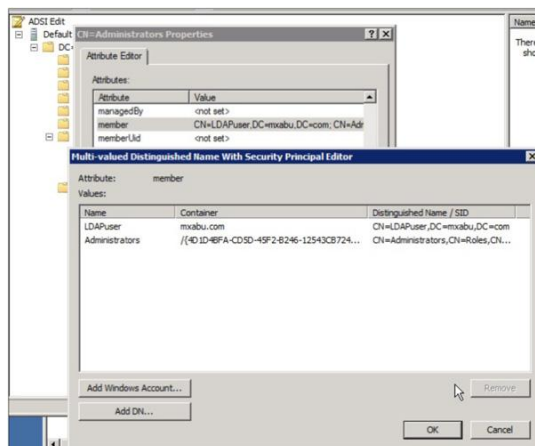
9. Choose **Edit** and change the value to **False**.



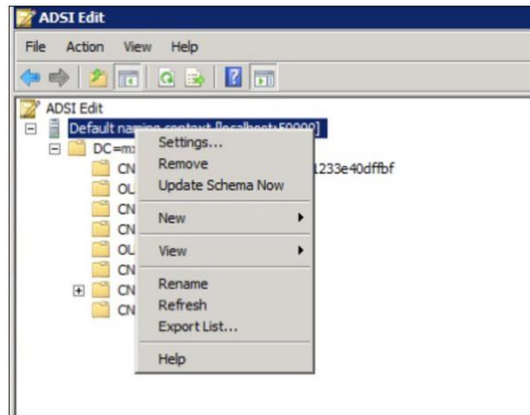
10. The new user needs to be added to one group that has read permission to the AD LDS. In this example, Administrators was chosen.
11. Browse to the **CN=Roles** container, right-click the **CN=Administrators** group, and choose **Properties**.



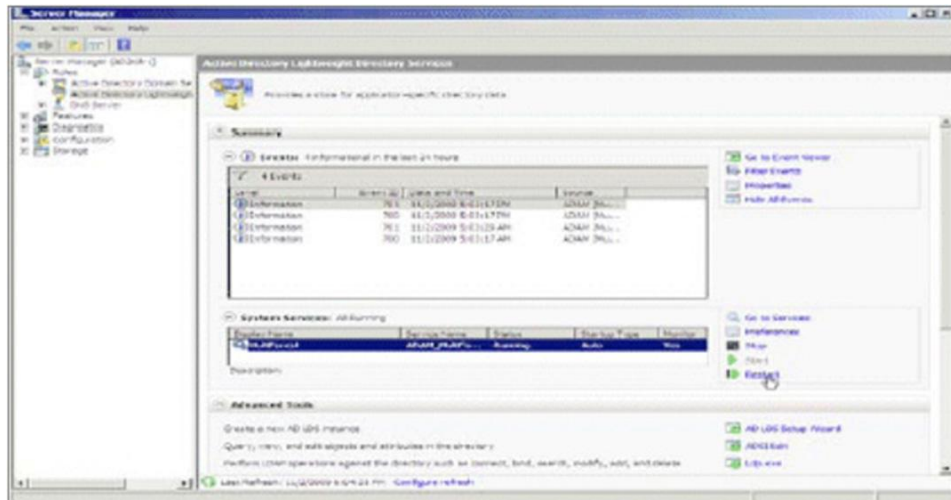
12. Browse to the member attribute and click **Edit**.



13. Add the new Distinguished Name (DN) that was previously created (for example, cn=LDAPuser,dc=mxabu,dc=com) to this group.
14. Update the schema.



15. Restart AD LDS.



8. 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 server that is running ADAM and on the server 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.

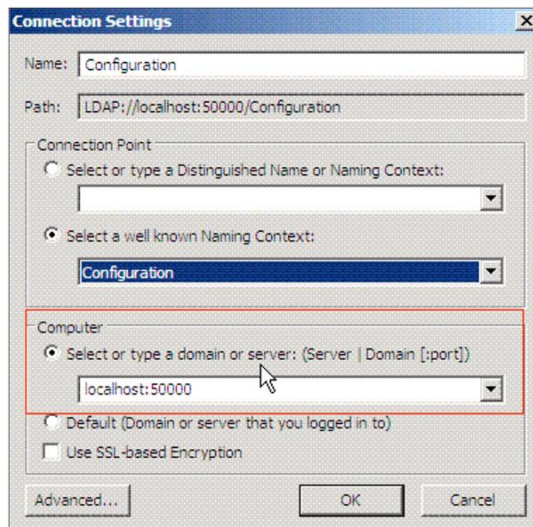
Note: Disabling the requirement for SSL for bind redirection causes the password of a Windows security principal to pass to the computer that is running ADAM without encryption. Thus, you should disable the SSL requirement only in a test environment.

By default, SSL is enabled. Perform these steps:

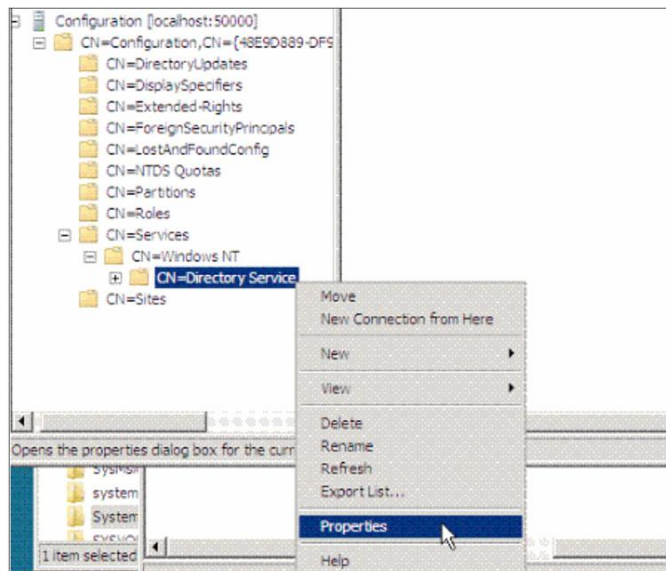
1. Generate the certificate for ADAM/AD LDS. Consult Microsoft documentation for information about ADAM/AD LDS certification generation.
2. Upload the ADAM/AD LDS certificate to the Cisco DMM for Show and Share®. Refer to the [User Guide for Cisco Digital Media Manager](#) on Cisco.com for more information.
3. Choose the checkbox to use SSL in the LDAP Directory page and the LDAP Authentication page.
4. Enter 50001 (in our example) for the LDAP port, which is the SSL port number given while installing the ADAM/AD LDS instance.

To disable the SSL requirement for bind redirection, perform these steps:

1. Click **Start**, point to **Administrative Tools**, and click **ADSI Edit**.
2. On the Action menu, choose **Connect to**.
3. Under computer, type **localhost:50000**, the host and port for ADAM.



4. Under Connection point, choose **Select a well-known Naming Context>Configuration** and then click **OK**.
5. In the console tree, browse to this container object in the configuration partition: CN=Windows NT,CN=Services.
6. Right-click **CN=Directory Service** and then choose **Properties**.



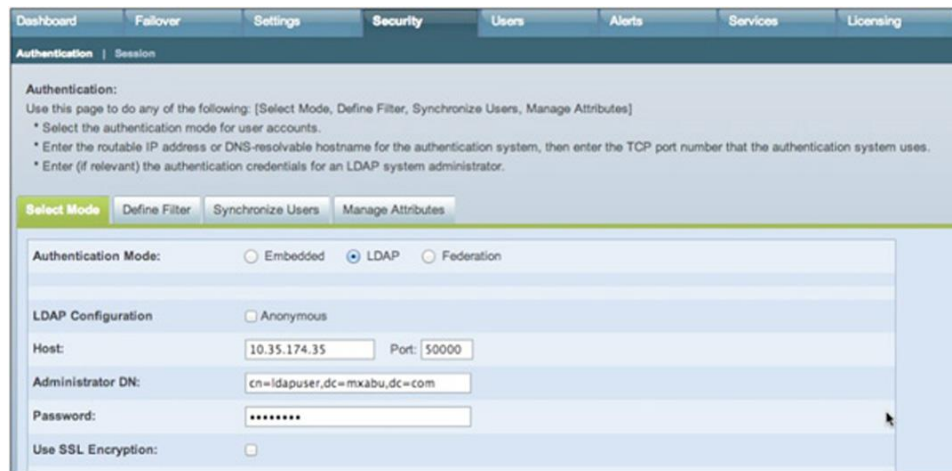
7. In Attributes, click **msDS-Other-Settings** and then click **Edit**.
8. In Values, click **RequireSecureProxyBind=1** and then click **Remove**.
9. In Value to add, type **RequireSecureProxyBind=0**, click **Add**, and then click **OK**.
10. Restart AD LDS for the changes to take effect.

For more information, refer to [Managing Authentication in ADAM](#) on Microsoft.com.

9. Configure DMM for Cisco Show and Share

Perform these steps:

1. Log in to DMM as superuser.
2. Choose **Administration>Security>Select Mode**.
3. Perform these steps to add the LDAP to the DMM:
 - a. For Authentication Mode, choose **LDAP**.
 - b. Add the Host: [*IP address of the LDS Server*] and Port: **50000**.
 - c. For Administrator DN, add: **cn=ldapuser,dc=mxabu,dc=com**.
 - d. Add the LDAPuser Password created in LDS.



The screenshot shows the DMM web interface with the 'Security' tab selected. Under the 'Authentication' section, the 'Select Mode' tab is active. The 'Authentication Mode' is set to 'LDAP'. The 'LDAP Configuration' section shows the following values: Host: 10.35.174.35, Port: 50000, Administrator DN: cn=ldapuser,dc=mxabu,dc=com, and Password: [masked]. The 'Use SSL Encryption' checkbox is unchecked.

4. Choose **Define Filter**.
 - a. Add a description to the filter.
 - b. For User Base DN, add: **ou=active,ou=mxabusers,dc=mxabu,dc=com**.
 - c. For User Filter, add: **objectClass=userProxy**.
 - d. Click **Validate** and then click **Add**.

For the icepg.com user, the filter would be similar to the following:

- a. Add a description to the filter.
- b. For User Base DN, add: **ou=activeusers,ou=icepgusers,dc=mxabu,dc=com**.
- c. For User Filter, add: **objectClass=userProxy**.
- d. Click **Validate** and then click **Add**.

LDAP Bookmarks | Scheduling

LDAP Bookmarks (saved list of query(ies) used to synchronize DMS to your LDAP server)

ID: 9	Description: MXABU Users	User Group Name: MXABU-Users
User Base DN: ou=active,ou=mxabu users,dc=mxabu,dc=com		
Filter: objectClass=userProxy		
Synchronization: <input type="radio"/> Initial <input checked="" type="radio"/> Update <input type="radio"/> Overwrite <input type="radio"/> Delete <input type="button" value="Submit"/> <input type="button" value="Cancel"/>		
ID: 10	Description: ICEPG Users	User Group Name: ICEPG-Users
User Base DN: ou=activeusers,ou=ICEPG Users,dc=mxabu,dc=com		
Filter: objectClass=userProxy		
Synchronization: <input type="radio"/> Initial <input checked="" type="radio"/> Update <input type="radio"/> Overwrite <input type="radio"/> Delete <input type="button" value="Submit"/> <input type="button" value="Cancel"/>		
ID: 12	Description: CTG Users	User Group Name: CTG-Users
User Base DN: ou=active,ou=ctg users,dc=mxabu,dc=com		
Filter: objectClass=userProxy		
Synchronization: <input type="radio"/> Initial <input checked="" type="radio"/> Update <input type="radio"/> Overwrite <input type="radio"/> Delete <input type="button" value="Submit"/> <input type="button" value="Cancel"/>		

The DMM has imported all users, and you can manage them now in Show and Share. For authentication, users will need to enter the same user ID and password that is in the original AD. Refer to the [Administrator Guide for Cisco Show and Share](#) on Cisco.com for more information.



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)