LDAP Directory on Yealink IP Phones

Introduction

LDAP stands for Lightweight Directory Access Protocol, which is a client-server protocol for accessing a directory service. LDAP is a directory service protocol that runs over TCP/IP. The nitty-gritty details of LDAP are defined in RFC 1777 "Lightweight Directory Access Protocol".

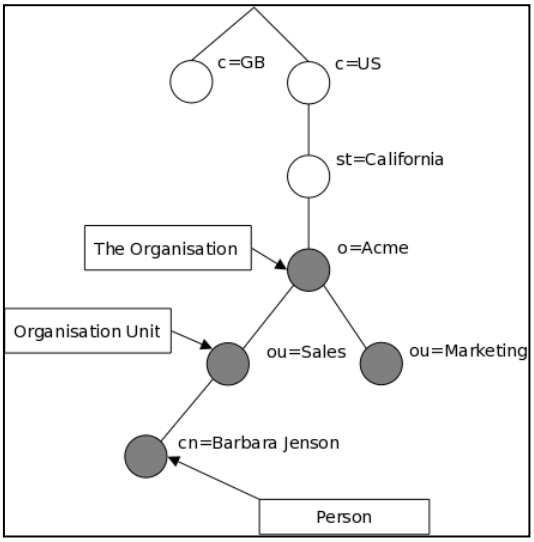
The following gives an overview of LDAP from a user's perspective.

What kind of information can be stored in the directory?

The LDAP information model is based on entries. An entry is a collection of attributes that has a globally-unique Distinguished Name (DN). The DN is used to refer to the entry unambiguously. Each of the entry's attributes has a type and one or more values. The types are typically mnemonic strings, like "cn" for the common name, or "mail" for the email address. The syntax of values depends on the attribute type. For example, a cn attribute might contain the value “Babs Jensen”. A mail attribute might contain the value "babs@example.com".

How is the information arranged?

In LDAP, directory entries are arranged in a hierarchical tree-like structure. Traditionally, this structure reflected the geographic and/or organizational boundaries. Entries representing countries appear at the top of the tree. Below them are entries representing states and national organizations. Below them might be entries representing organizational units, people, printers, documents, or just about anything else you can think of. The following shows an example of an LDAP directory tree using traditional naming.



LDAP enables you to locate organizations, individuals, and other resources such as files and devices in a network, whether on the Internet or a corporate intranet, and whether or not you know the domain name, IP address, or geographic whereabouts. An LDAP directory can be

distributed among many servers on a network, then replicated and synchronized regularly. LDAP is particularly useful for storing information that you wish to read from many locations, but update infrequently.

This guide provides configurations on the LDAP server and IP phones, and applies to the following Yealink IP phones:

- CP860 IP phones running firmware version 71 or later
- SIP-T48G, SIP-T46G, SIP-T42G and SIP-T41P IP phones running firmware version 73 or later
- SIP-T58A, SIP VP-T49G, SIP-T40P, SIP-T29G, SIP-T23P/G, SIP-T21(P) E2, CP960 and W56P IP phones running firmware version 80 or later
- SIP-T48S, SIP-T46S, SIP-T42S, SIP-T41S, SIP-T40G, SIP-T27G, SIP-T19(P) E2, CP920, W60P and W52P IP phones running firmware version 81 or later
- VP59, W53P and CP930W-Base IP phones running firmware version 83 or later
- SIP-T57W, SIP-T54W, SIP-T53W, SIP-T53, SIP-T48U, SIP-T46U and SIP-T43U IP phones running firmware version 84 or later
- SIP-T44W, SIP-T44U, SIP-T34W, and T31W IP phones running firmware version 86 or later
- SIP-T88V Pro, SIP-T88W(Pro), SIP-T87W, SIP-T85W, SIP-T77U, SIP-T74W, SIP-T74U, SIP-T73W, and SIP-T73U IP phones running firmware version 87 or later

Installing and Configuring the LDAP Server

An LDAP server is essentially a bit like an SQL server, which is mainly used for storing/retrieving information about people (such as contacts). The configuration settings on the phone will be altered depending on how the LDAP server is configured.

Before using the LDAP feature on IP phones, you must make sure the LDAP server is prepared properly, otherwise, you need to install and configure an LDAP server. This chapter shows you how to install and configure an LDAP server. We recommend you to use the OpenLDAP, Microsoft Active Directory, Microsoft Active Directory Application Mode (ADAM) or Sun One Directory Server on Windows system.

OpenLDAP

Installing the OpenLDAP Server

This section shows you how to install an OpenLDAP server on Microsoft Windows 2007 system. The OpenLDAP server software is available for free. You can download it from http://www.userbooster.de/en/download/openldap-for-windows.aspx?l=en.

To install the OpenLDAP server:

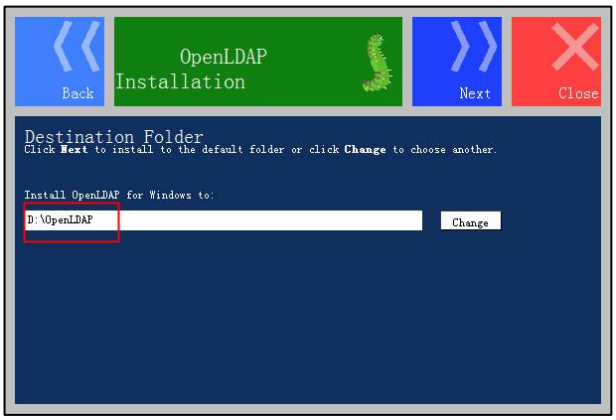
1. Double click the OpenLDAP application to start the installation. You will be prompted for the installation.

2. Click **Yes** to continue the installation.
3. Follow the default settings and click **Next** until the **Destination Folder** screen appears.

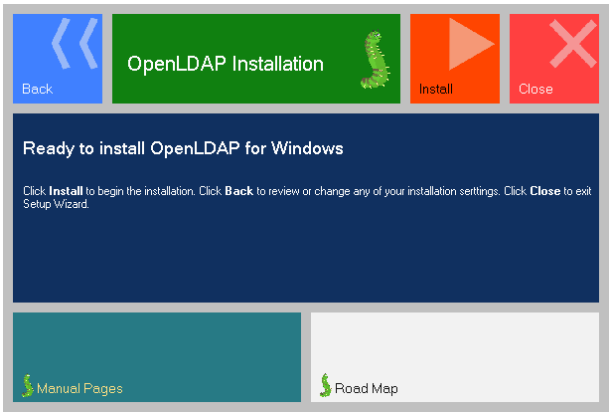
4. Click **Change** to locate the installation path from the local computer system and then click **Next**.

   You need to remember the installation path (e.g., D:\OpenLDAP) located here.

   The screenshot for reference is shown as below:



5. Follow the default settings and click **Next** until the **Ready to install OpenLDAP for Windows** screen appears.



6. Click **Install** to start the installation.
7. Click **Close** to exit the Setup Wizard.

For more information on how to install the OpenLDAP server for windows, refer to the website online:

http://www.userbooster.de/en/support/feature-articles/openldap-for-windows-installation.aspx

.

Configuring the OpenLDAP Server

Editing the slapd.conf File

Access the OpenLDAP installation path. Edit the manager information for LDAP.

1. Open and edit the slapd.conf file using your favorite text editor.

   Find the commands

   Suffix "dc=maxcrc, dc=com"

   Rootdn "cn=Manager,dc=maxcrc,dc=com"

   Suffix defines the components of the domain name.

   Rootdn defines the manager as a management user for accessing the LDAP server.

   For example:

   Suffix "dc=yealink,dc=com"

   Rootdn "cn=Manager,dc=yealink,dc=com "

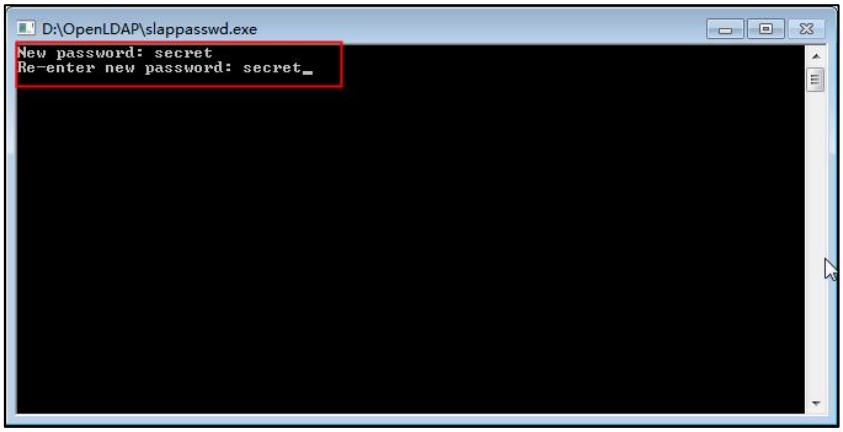
   The suffix line means that the domain name of the LDAP directory is yealink.com. The Rootdn line defines a management user named as Manager.

   If the domain name contains additional components, for example, yealink.com.cn, the suffix line will be edited as below:

   Suffix "dc=yealink,dc=com,dc=cn"

   Rootdn "cn=Manager,dc=yealink,dc=com,dc=cn"

2. Double click slappasswd.exe to modify the user password for the management user. Type the new password twice.



Starting the Slapd Service

To start the slapd service:

1. Click **Start**->**Run**.
2. Enter **cmd** in the pop-up dialogue box and click **OK** to enter the command line interface.
3. Access the server installation path. For example, execute the following commands to access

the server installation path at **D:\OpenLDAP**.

```
C:\Users\yl0215>d:

D:\>cd OpenLDAP

D:\OpenLDAP>_
```

4. Execute the command **slapd.exe -d 1 -f ./slapd.conf** to start the slapd service.

```
C:\Users\yl0215>d:

D:\>cd OpenLDAP

D:\OpenLDAP>slapd.exe -d 1 -f ./slapd.conf_
```

If the service runs successfully, you can find the prompt "**slapd starting**".

The screenshot for reference is shown as below:

```
C:\Windows\system32\CMD.exe - slapd.exe  -d 1 -f ./slapd.conf
5498d32e config_build_entry: "cn=schema"
5498d32e >>> dnNormalize: <cn={0}core>
5498d32e <<< dnNormalize: <cn={0}core>
5498d32e config_build_entry: "cn={0}core"
5498d32e >>> dnNormalize: <cn={1}cosine>
5498d32e <<< dnNormalize: <cn={1}cosine>
5498d32e config_build_entry: "cn={1}cosine"
5498d32e >>> dnNormalize: <cn={2}nis>
5498d32e <<< dnNormalize: <cn={2}nis>
5498d32e config_build_entry: "cn={2}nis"
5498d32e >>> dnNormalize: <cn={3}inetorgperson>
5498d32e <<< dnNormalize: <cn={3}inetorgperson>
5498d32e config_build_entry: "cn={3}inetorgperson"
5498d32e config_build_entry: "olcDatabase={-1}frontend"
5498d32e config_build_entry: "olcDatabase={0}config"
5498d32e config_build_entry: "olcDatabase={1}bdb"
5498d32e backend_startup_one: starting "dc=yealink,dc=com"
5498d32e bdb_db_open: warning - no DB_CONFIG file found in directory ./data: (2)
.
Expect poor performance for suffix "dc=yealink,dc=com".
5498d32e bdb_db_open: database "dc=yealink,dc=com": dbenv_open(./data).
5498d32f bdb_monitor_db_open: monitoring disabled; configure monitor database to
 enable
5498d32f slapd starting
```

Please do not close this window to make sure the LDAP server keeps running.

Adding the Initial Entry to the LDAP Directory

You can add the initial entry to the LDAP directory by using the LDIF file. Create a new text document, then modify the filename extension as ldif and place the document to the OpenLDAP installation path. For example, create a text document named as test.txt, right-click the test.txt document and then select to rename it, modify the filename extension as ldif. Open the LDIF file with your favorite text editor and input the corresponding content. The following shows an example of the content of the LDIF file:

dn: dc=yealink,dc=com

objectClass: top

objectClass: dcObject

objectClass: domain

dc: yealink

```
dn: ou=roles,dc=yealink,dc=com
objectClass: top
objectClass: organizationalUnit
ou: roles

dn: ou=people,dc=yealink,dc=com
objectClass: top
objectClass: organizationalUnit
ou: people

dn: cn=Test Users,ou=roles,dc=yealink,dc=com
objectClass: groupOfUniqueNames
cn: Test Users
uniqueMember:
uid=sspecial,ou=people,dc=yealink,dc=com
uniqueMember:
uid=jbloggs,ou=people,dc=yealink,dc=com

dn: cn=Special Users,ou=roles,dc=yealink,dc=com
objectClass: groupOfUniqueNames
cn: Special Users
uniqueMember:
uid=sspecial,ou=people,dc=yealink,dc=com

dn: cn=Admin Users,ou=roles,dc=yealink,dc=com
objectClass: groupOfUniqueNames
cn: Admin Users
uniqueMember:
uid=admin,ou=people,dc=yealink,dc=com

dn: uid=admin,ou=people,dc=yealink,dc=com
objectClass: person
objectClass: inetOrgPerson
cn: State App
displayName: App Admin
givenName: App
mail: admin@fake.org
```

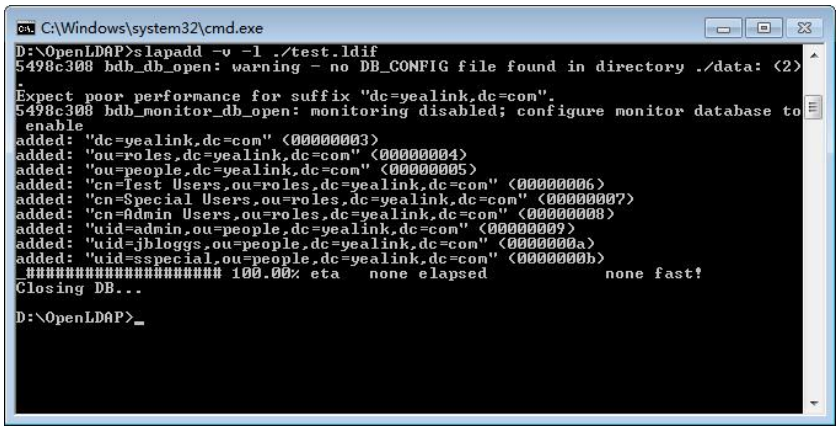
```
sn: Admin
uid: admin
userPassword: adminpassword

dn: uid=jbloggs,ou=people,dc=yealink,dc=com
objectClass: person
objectClass: inetOrgPerson
cn: Joe Bloggs
displayName: Joe Bloggs
givenName: Joe
mail: jbloggs@fake.org
sn: Bloggs
uid: jbloggs
userPassword: password

dn: uid=sspecial,ou=people,dc=yealink,dc=com
objectClass: person
objectClass: inetOrgPerson
cn: Super Special
displayName: Super Special
givenName: Super
mail: sspecial@fake.org
sn: Special
uid: sspecial
userPassword: password</span>
```

To add the initial entry using the test.ldif file:

1. Click **Start**->**Run**.
2. Execute **cmd** in the pop-up dialogue box and click **OK** to enter the command line interface.
3. Access the server installation path. For example, execute the following commands to access the server installation path at **D:\OpenLDAP**.

4. Execute the command **slapadd -v -l ./test.ldif** to add the initial entry.

   The screenshot for reference is shown as below:



Configuring the LDAPExploreTool2

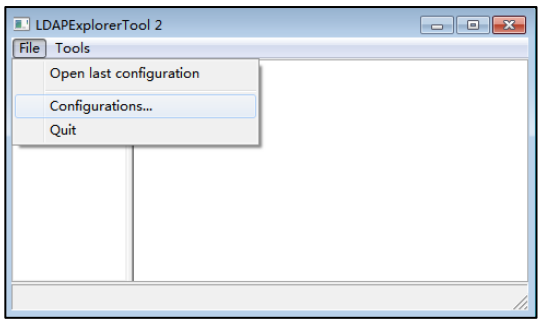
The LDAPExploreTool2 application supports running on the Windows system. The application is a graphical LDAP tool that enables you to browse, modify and manage contact entry on the LDAP server.

If you have an LDAPExploreTool2 application installed on your computer, open it now, otherwise, download the application from http://ldaptool.sourceforge.net/. And then complete the installation following the wizard.

Creating a Configuration

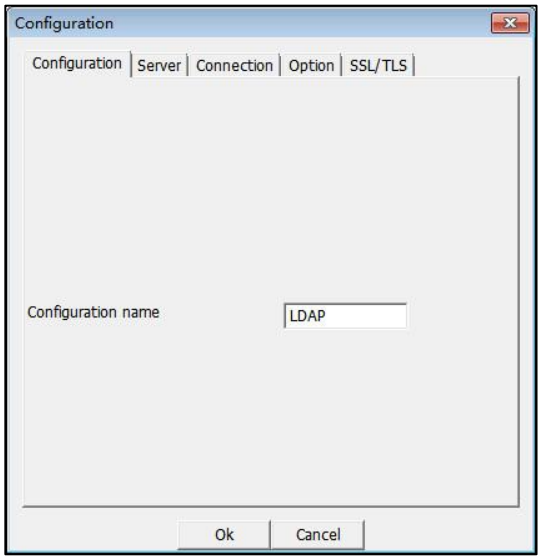
To create a configuration:

1. Double click the LDAPExploreTool2.exe to run the application.
2. Click **File**->**Configurations**.

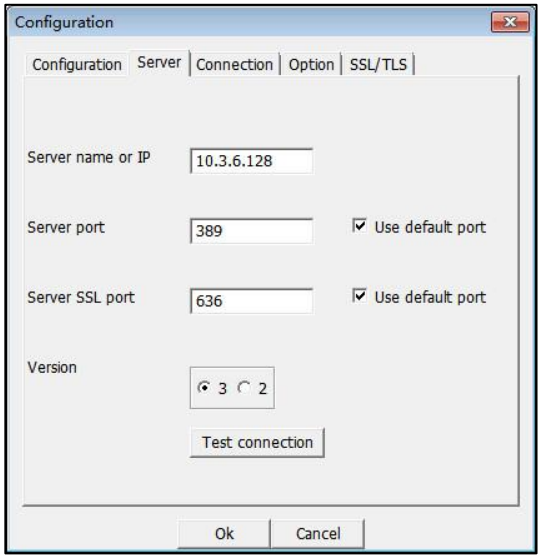


3. Click **New** to create a new configuration.

4. Enter a name in the **Configuration name** field under the **Configuration** tab.



5. Enter the domain name or IP address of the LDAP server in the **Server name or IP** field under the **Server** tab. Check the checkbox of **Use default port** for the **Server port** and **Server SSL port**.



6. Enter the user DN and password in the **User DN** and **Password** field under the **Connection** tab.

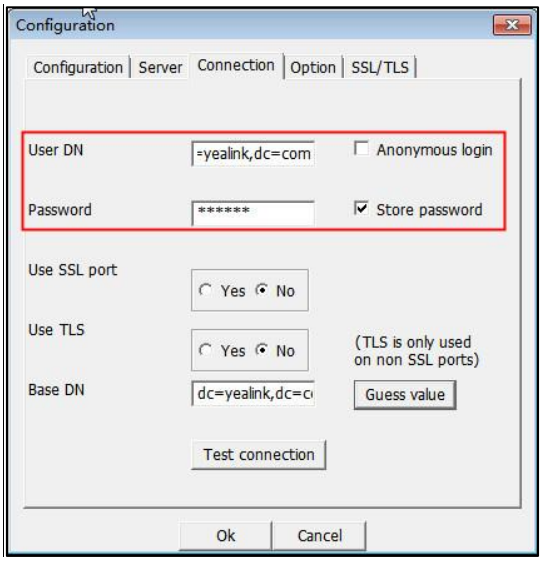
   The user DN and password correspond with the Rootdn and Rootpw defined in the slapd.conf file.

   For example, according to the manager information defined in the slapd.conf file:

   Rootdn "cn=Manager,dc=yealink,dc=com"

   Rootpw secret

Enter **cn=Manager,dc=yealink,dc=com** in the **User DN** field and **secret** in the **Password** field under the **Connection** tab.

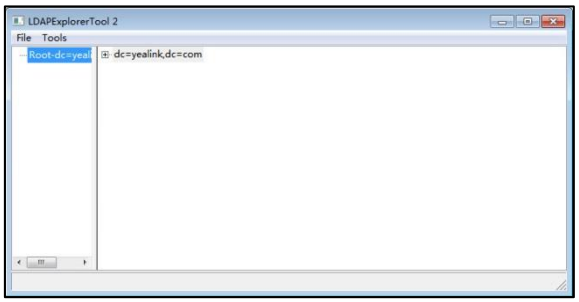


7. Click **Guess value** to fill the **Base DN** automatically.
8. Click **Test connection** to test the connection to the LDAP server. If you encounter an error or warning during the test, you need to resolve the error or warning first according to the prompt, and then retry to test the connection.
9. Click **OK** to accept the change.

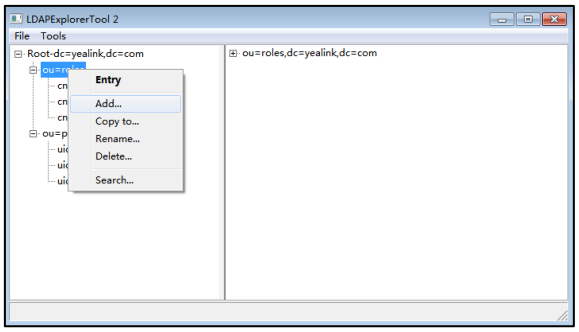
Adding Entries

To add entries:

1. Click **File**->**Configurations**, select the configuration created above, and then click **Open**. The screenshot for reference is shown as below:



2. Right-click the root entry, and then select **Add** to add a new entry.



3. Enter the desired values in the corresponding fields.

   Parent DN: It will be automatically generated according to the server configuration.

   Entry RDN: The format is cn=XXX. This is a unique identifier for each entry.

   Object Class (from schema): Select the structure class which the entry belongs to. Each structure class has its must attributes and may attributes. For example, we select **person** from the **Object class (from schema)** drop-down menu.

4. Select the desired attributes for the object class.

   Must attributes: Double click attributes to add them to the entry node. All attributes listed in the **Must attributes** field must be added and each value of the attribute must be set.

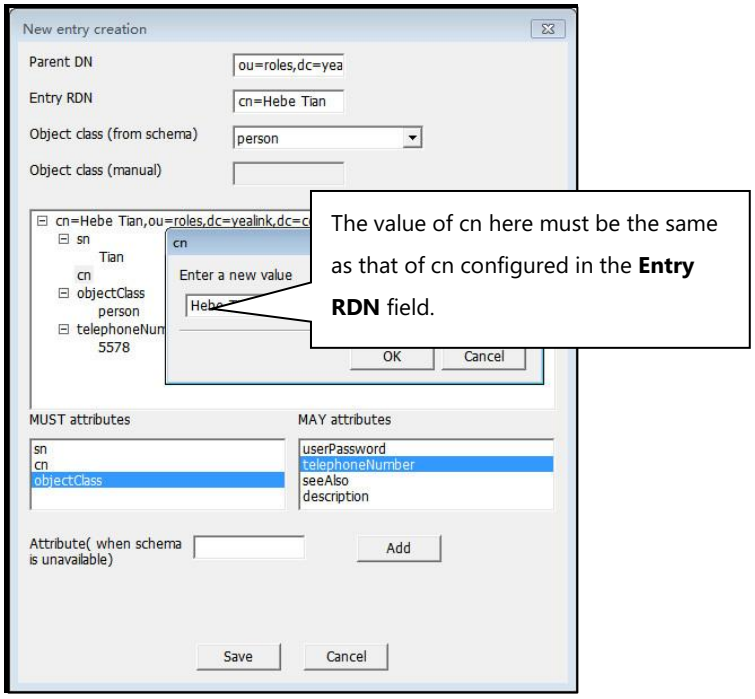
   May attributes: Double click the desired attributes to add them to the entry node. The attributes listed in the **May attributes** field are optional.

   Common attributes are listed in the following table:

Attribute	Name	Description
cn	commonName	Full name of the entry.
gn	givenName	The first name also called Christian name.
sn	surname	Surname, last name or family name.
telephoneNumber	telephoneNumber	Office phone number.
homePhone	homeTelephoneNumber	Home phone number.
mobile	mobileTelephoneNumber	Mobile or cellular phone number.
pager	pagerTelephoneNumber	Pager telephone number.
company	company	Company name.
o	organizationName	Organization name.
ou	organizationlUnitName	Usual department or any sub entity of larger entity.

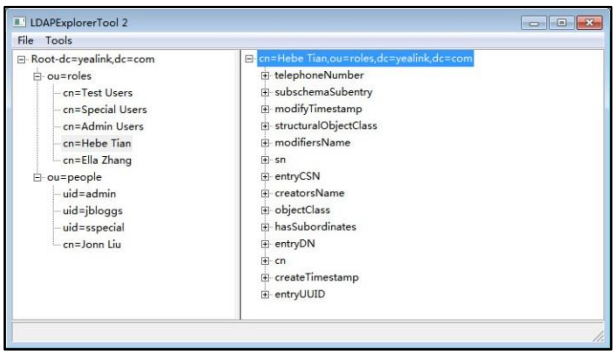
5. Right-click the selected attribute and then select **Add value**.

The screenshot of adding a new entry is shown as below:



6. Click **Save** to confirm the configuration.
7. Repeat steps 2 to 6 to add more contact entries.

   You can find the added entries at the left of the LDAP catalog.



Microsoft Active Directory

Installing the Microsoft Active Directory Domain Services

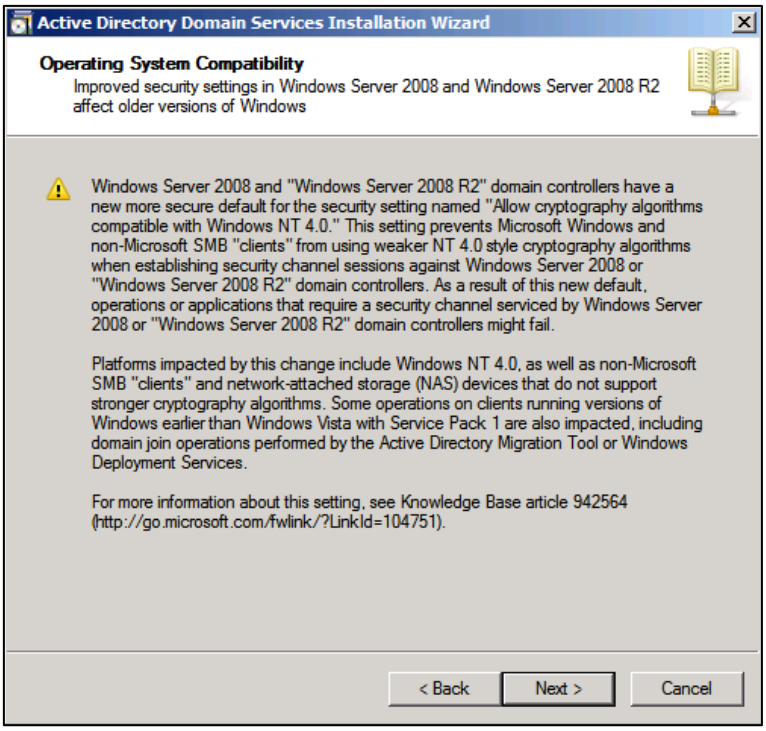
This section shows you how to install an active directory on Microsoft Windows Server 2008 R2 Enterprise 64-bit system.

To install the Microsoft Active Directory Domain Services:

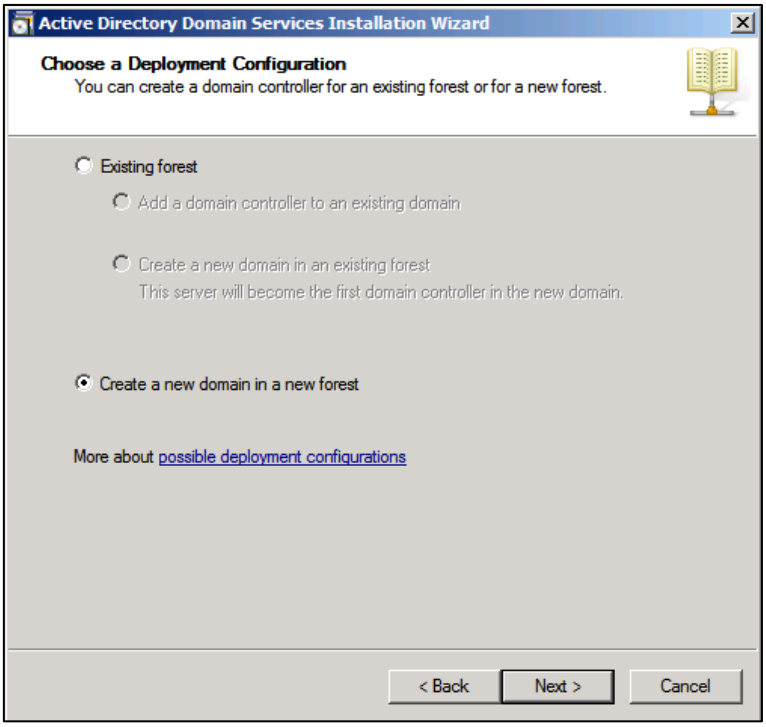
1. Click **Start**->**Run**.
2. Enter **dcpromo** in the pop-up dialogue box and click **OK**.

3. The Active Directory Domain Services Installation Wizard will appear after a short while, click **Next**.

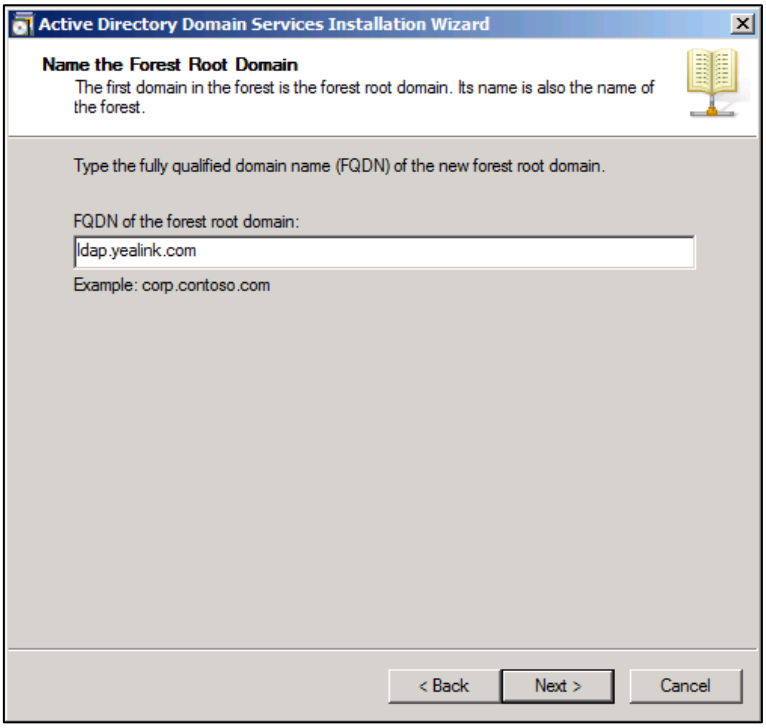
4. Read the provided information and click **Next**.



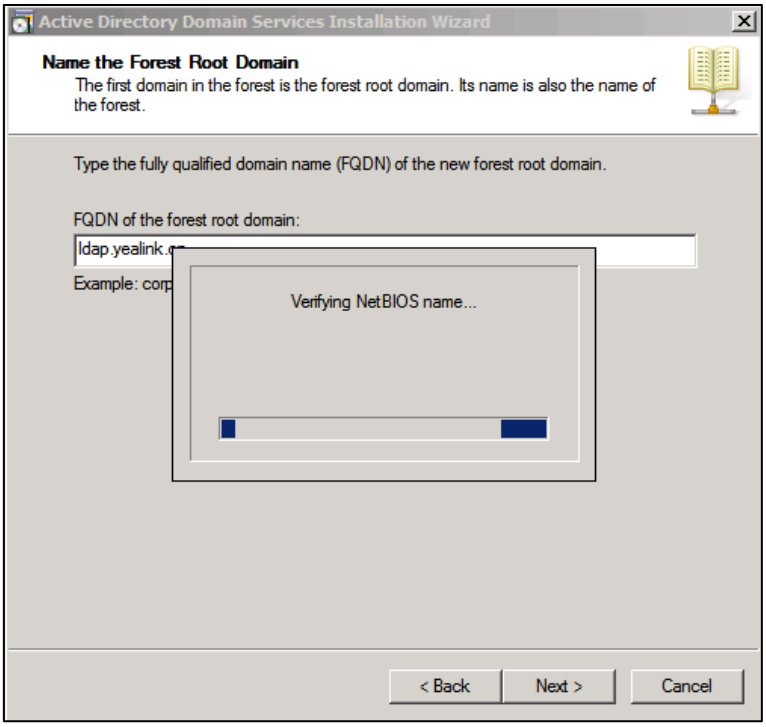
5. Mark the **Create a new domain in a new forest** radio box and click **Next**.



6. Enter an appropriate domain name for the forest root domain and click **Next**.

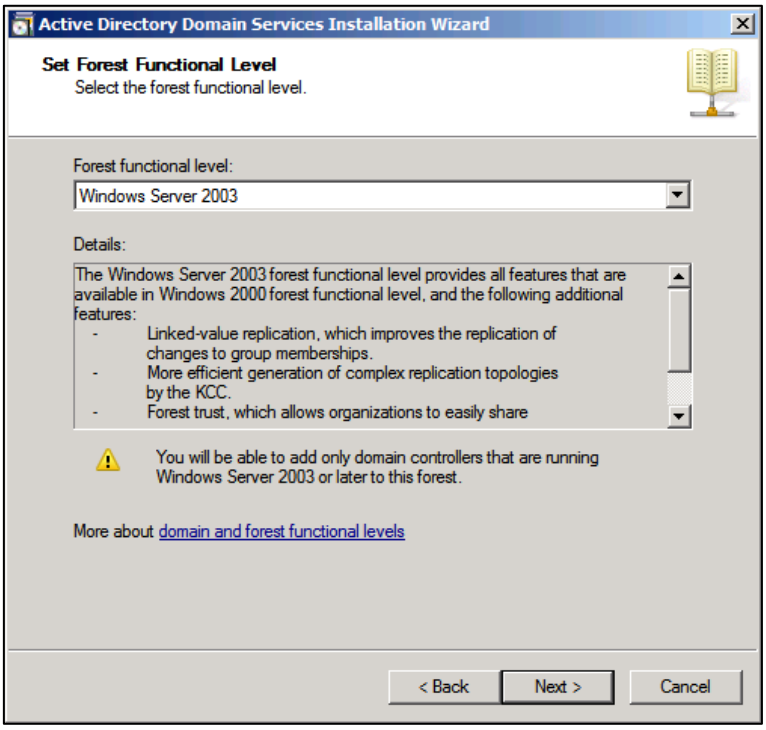


The wizard will check if the domain name is in use on the local network.



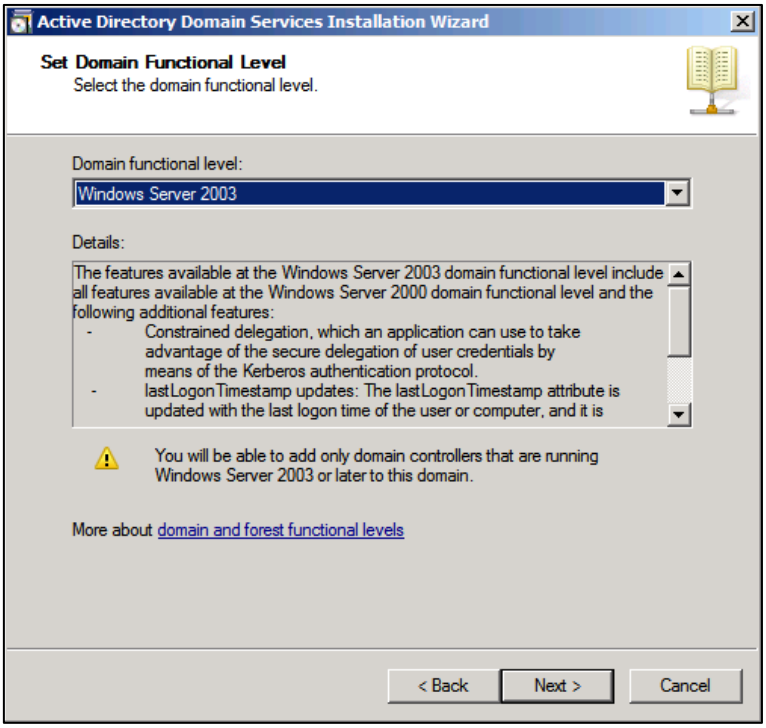
7. Select the desired forest functional level from the **Forest functional level** drop-down menu, and click **Next**.

   For more information, click **domain and forest functional levels**.



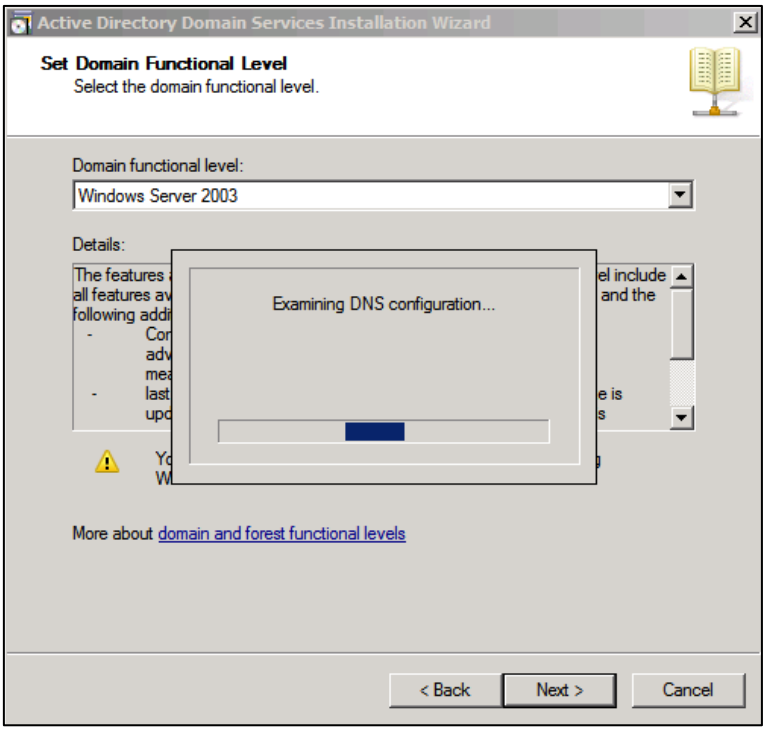
8. Select the desired domain functional level from the **Domain functional level** drop-down menu, and click **Next**.

For more information, click **domain and forest functional levels**.

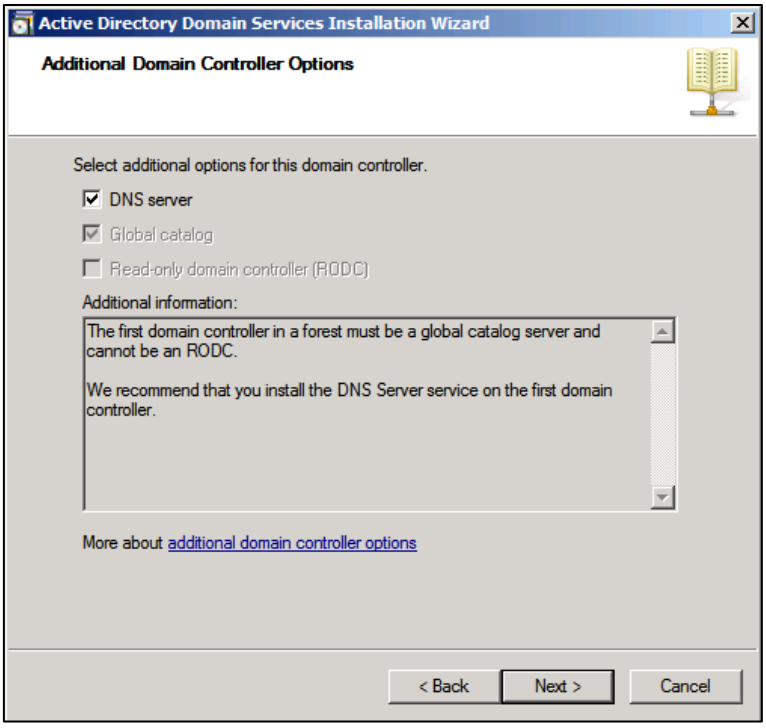


If you select **Windows Server 2008 R2** for the forest functional level, you will not be prompted to select a domain functional level.

The wizard will check if the DNS is properly configured on the local network.

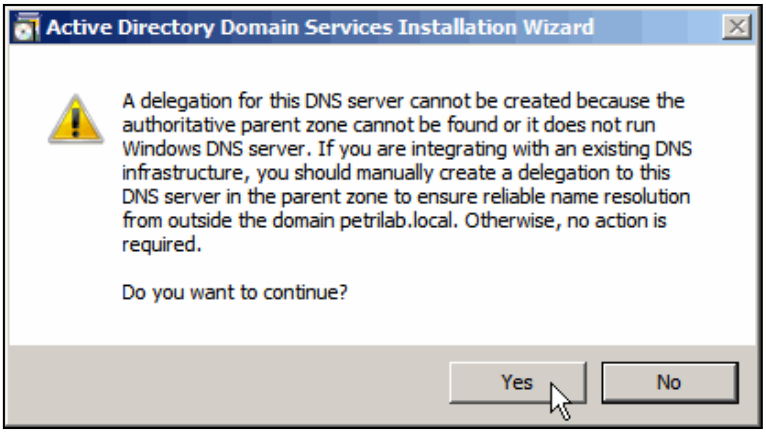


9. Select additional options for this domain controller if required, and click **Next**.



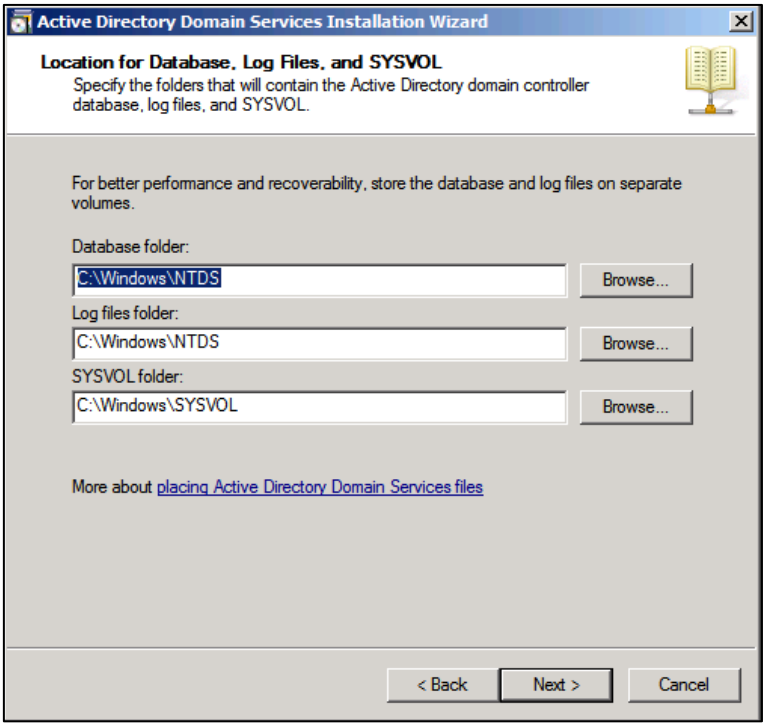
You may get a warning telling you that the server has one or more dynamic IP addresses. We recommend assigning a static IP address to the server.

10. The wizard will prompt a warning about DNS delegation. Since no DNS has been configured yet, you can ignore the message and click **Yes**.



11. Specify the desired paths for the database, log files, and SYSVOL folders, and click **Next**.

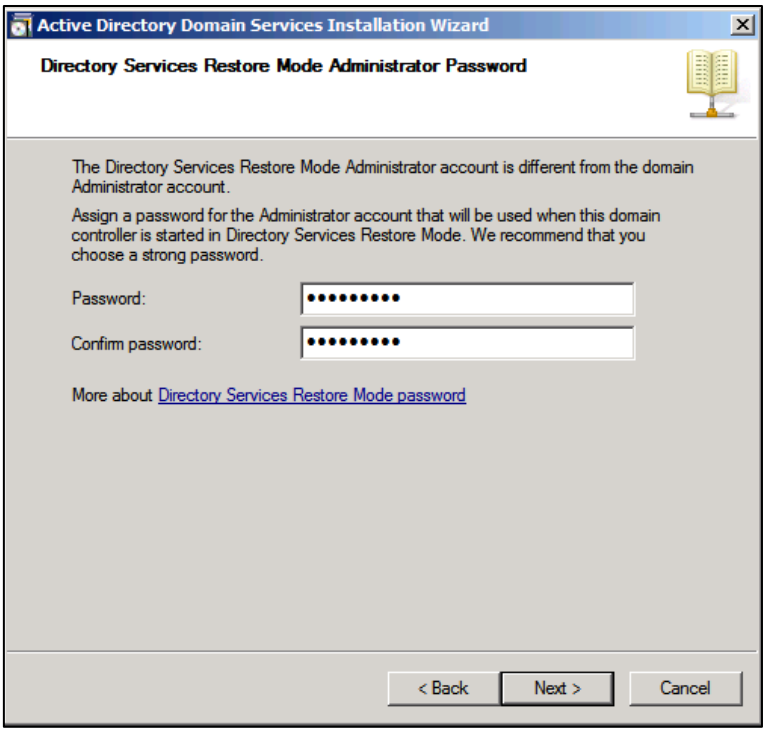
For more information, click **placing Active Directory Domain Services files**.



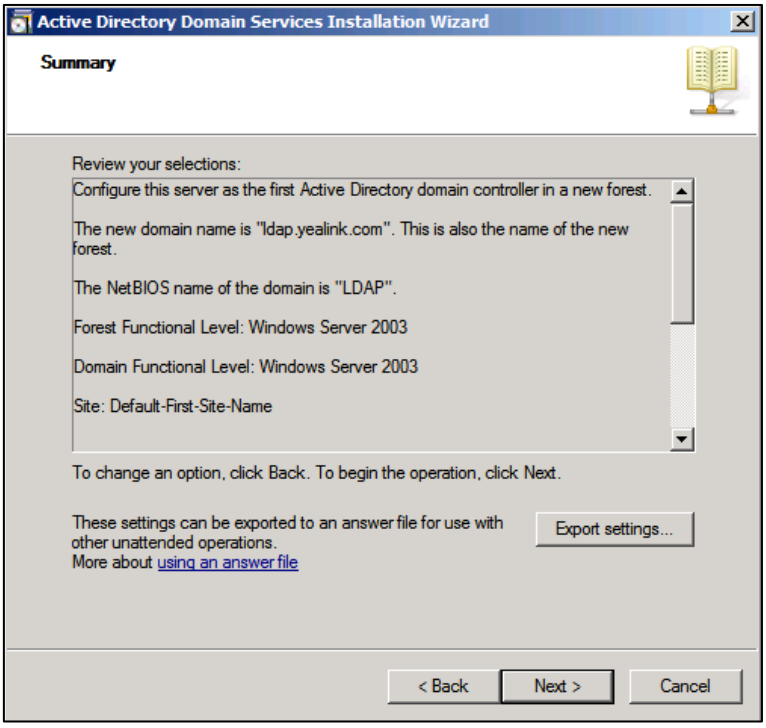
12. Configure the password for the active directory recovery mode, and click **Next**.

For more information, click **Directory Services Restore Mode password**.

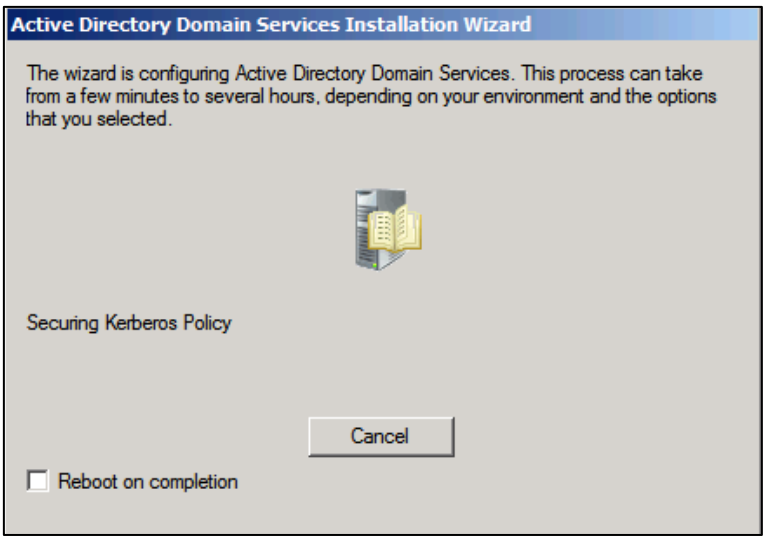
The password should be complex and at least 7 characters long.



13. Review your selection and click **Next**.



The wizard will prompt that the system begins to create the Active Directory Domain Services.



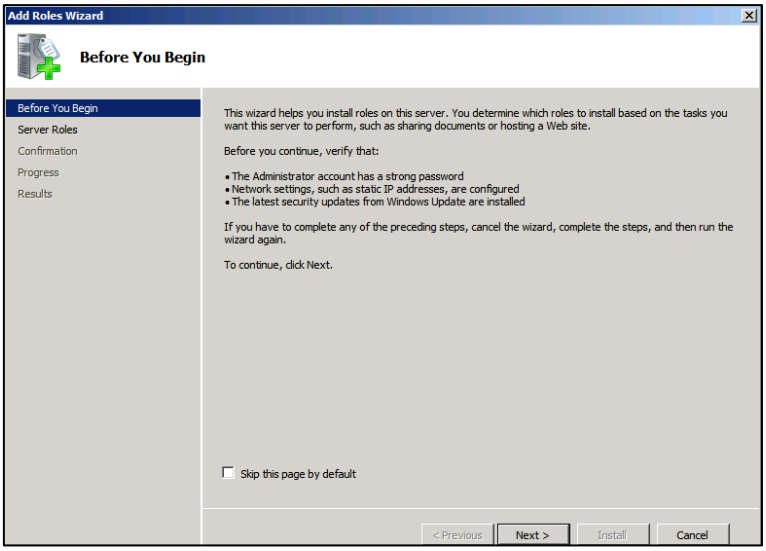
14. Click **Finish** to complete the installation and exit the wizard.

Installing Active Directory Lightweight Directory Services Role

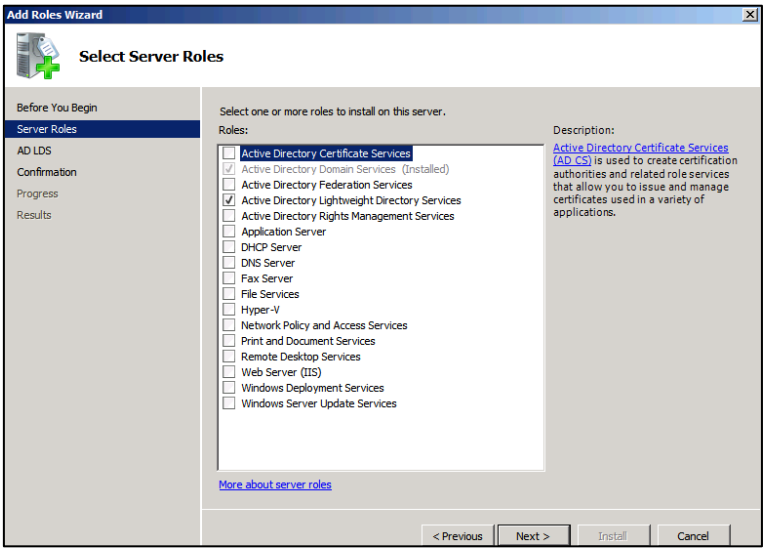
You should also install the Active Directory Lightweight Directory Services role on the Windows Server 2008 system.

To install the Active Directory Lightweight Directory Services role:

1. Click **Start**->**Administrative Tools**->**Server Manager**.
2. Right-click **Roles**, and then select **Add Roles**.
3. The Add Roles Wizard will pop up, click **Next**.

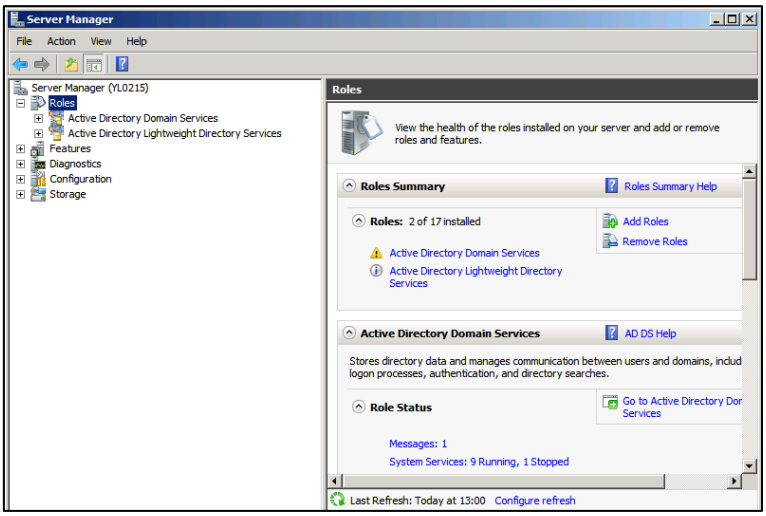


4. Check the **Active Directory Lightweight Directory Services** checkbox and click **Next**.



5. Follow the default settings and click **Next**.
6. When the installation is completed, click **Close**.

   After the installation succeeds, you will find the **Active Directory Lightweight Directory Services** role listed in the roles of the server manager.



Configuring the Microsoft Active Directory Server

Adding an Entry to the Active Directory

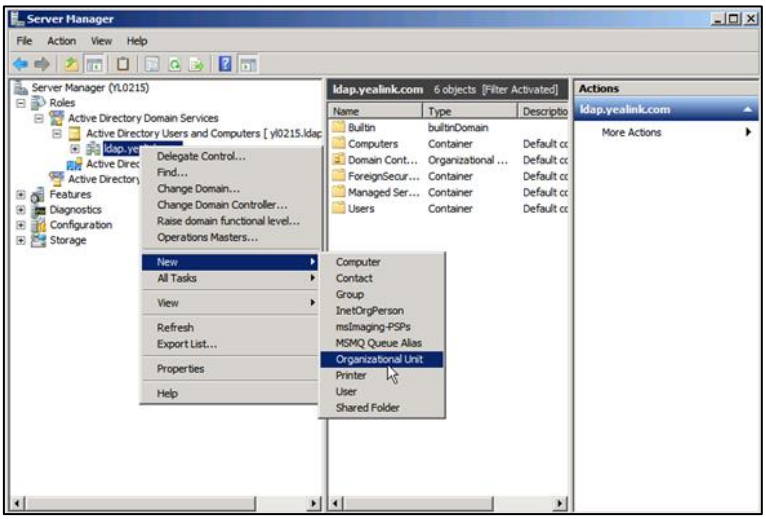
You can add entries to the active directory one by one in this way.

To add an entry to the Active Directory:

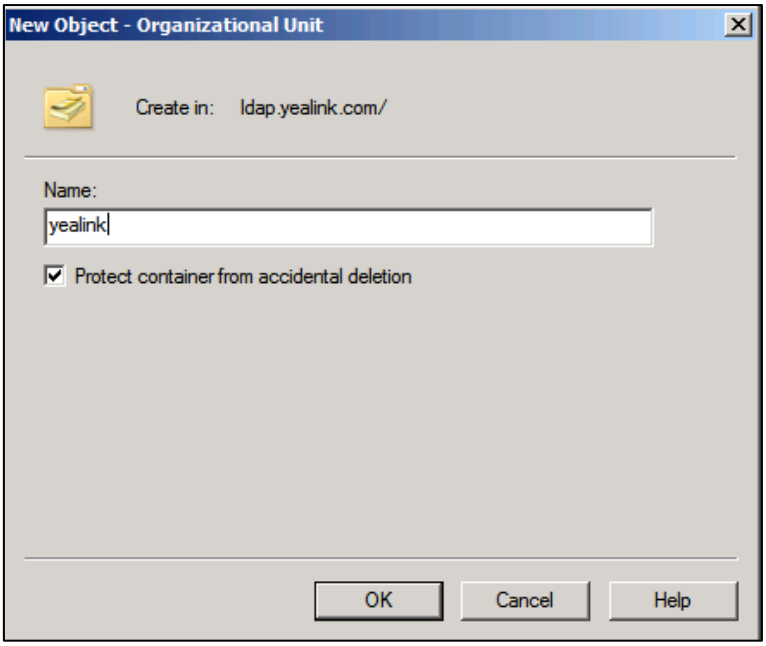
1. Click **Start**->**Administrative Tools**->**Server Manager**.
2. Double click **Roles**->**Active Directory Domain Services**->**Active Directory Users and**

Computers.

3. Right-click the domain name created above (e.g., ldap.yealink.com), and then select **New**->**Organizational Unit**.

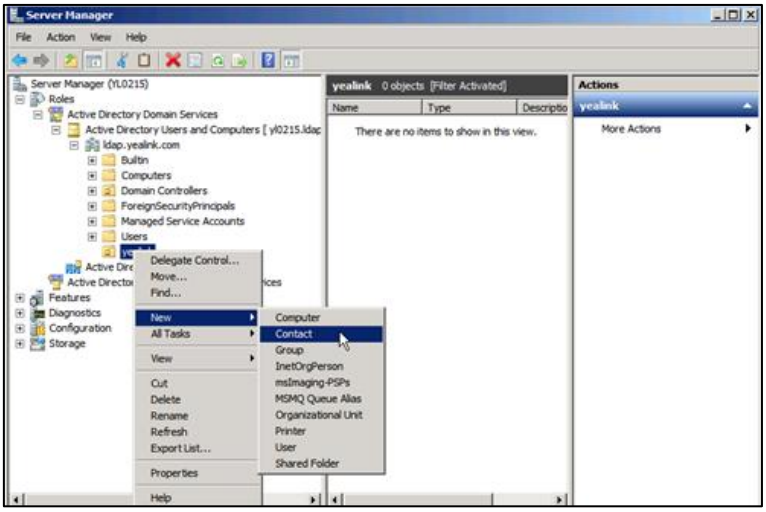


4. Enter the desired name of the organizational unit.

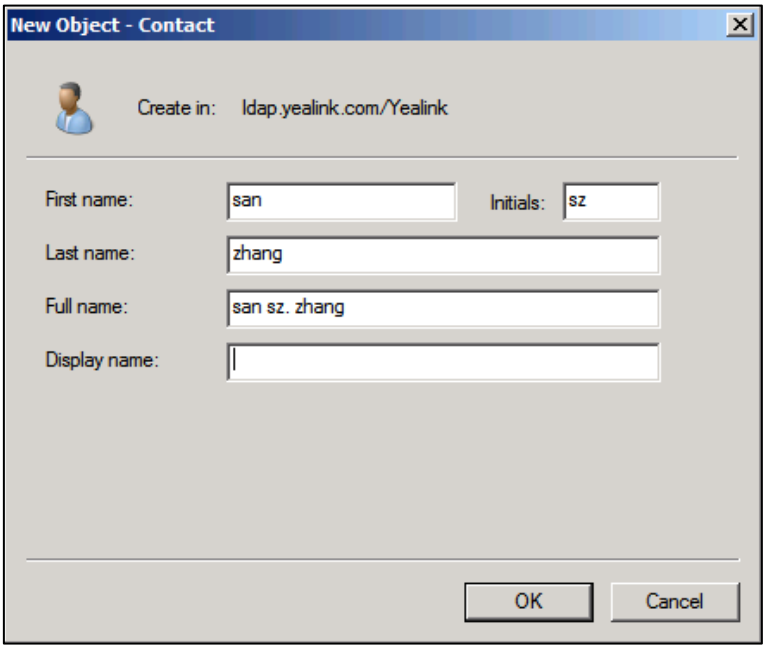


5. Click **OK** to accept the change.

6. Right-click the organizational unit created above, and then select **New**->**Contact**.



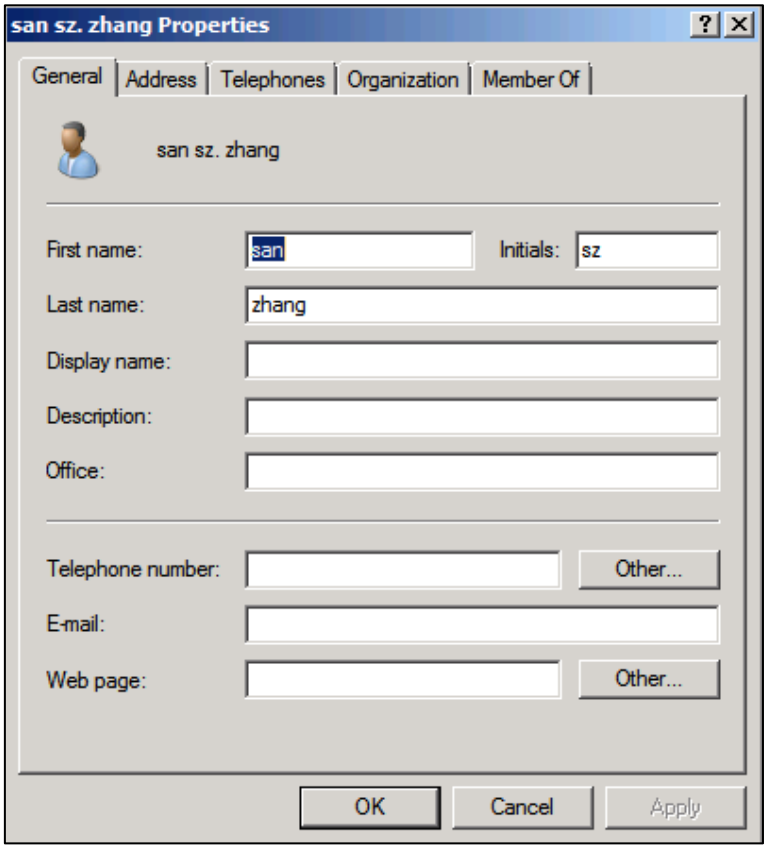
7. Enter the desired values in the corresponding fields.



8. Click **OK** to accept the change.

9. Double click the contact created above.

10. Configure more properties of the contact.



11. Click **OK** to accept the change.

Adding Entries to the Active Directory Using the ldifde Tool

You can use an LDIF file to perform a batch import of all entries to the active directory.

To create the LDIF file:

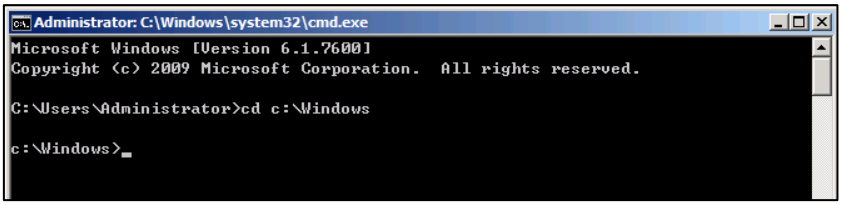
Create a new text document and then modify the filename extension as ldif. For example, create a text document named as test.txt, right-click the test.txt document and then select to rename it, modify the filename extension as ldif. Open the LDIF file with your favorite text editor and input the corresponding content. The following shows an example of the content of the LDIF file:

```
##Create a new organizational unit##
dn: OU=yealink,DC=ldap,DC=yealink,DC=com
changetype: add
objectClass: top
objectClass: organizationalUnit
ou: yealink
name: yealink

##create a new contact##
dn: CN=san zhang,OU=yealink,DC=ldap,DC=yealink,DC=com
changetype: add
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: contact
cn: san zhang
sn: zhang
givenName: san
initials: zs
name: san zhang
ipPhone: 2336
mobile: 15557107369
```

To import the test.ldif file:

1. Click **Start**->**Run**.
2. Enter **cmd** in the pop-up dialogue box and click **OK** to enter the command line interface.

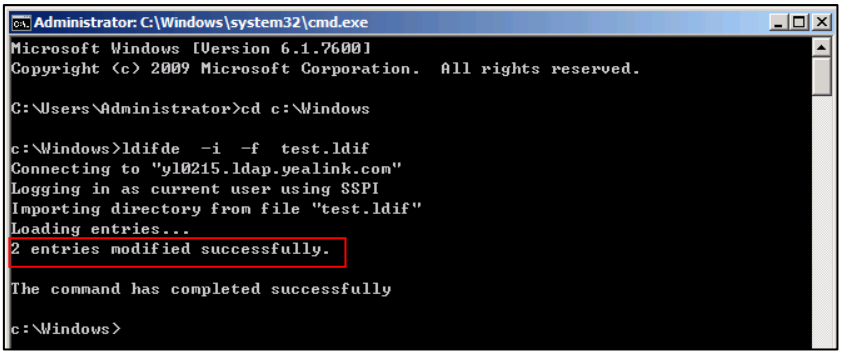
3. Execute the command **cd** to access the path of the test.ldif file. For example, execute **cd c:\Windows** to access the path of the test.ldif file at **c:\Windows**.



4. Execute the command **ldifde -i -f test.ldif** to import the file.

   If the entries are added successfully, you can find the prompt "**n entries modified successfully**" ("n" indicates the number of the added entries).

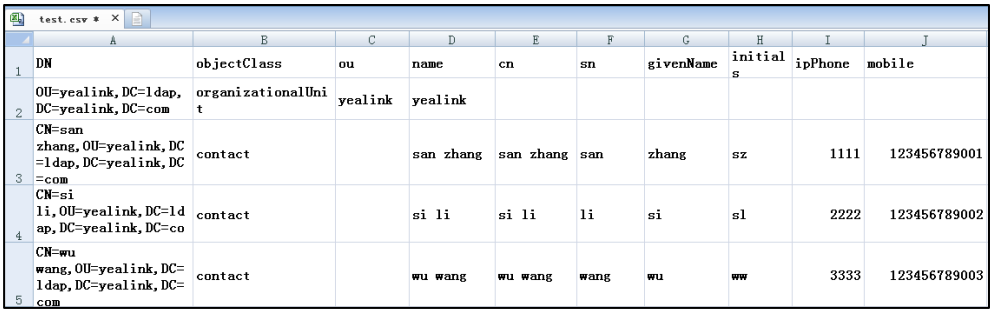
   The screenshot for reference is shown as below:



You can also export the existing entries on the active directory into a *.ldif file first, modify the file, and then import the modified file into the active directory. For more information, refer to the network resource.

Adding Entries to the Active Directory Using the Csvde Tool

You can also use a CSV file to perform a batch import of all entries to the active directory. Create a new document using a spreadsheet application (e.g., Microsoft Excel) and then save the document to your local computer using "Save as" in the format "*.csv". For example, create a document named as test.xls, click "Save as" to save the document as test.csv. Open the CSV file with the spreadsheet application and input the corresponding content. The following shows an example of the CSV file content:



	A	B	C	D	E	F	G	H	I	J
1	DN	objectClass	ou	name	cn	sn	givenName	initials	ipPhone	mobile
2	OU=yealink,DC=ldap,DC=yealink,DC=com	organizationalUnit	yealink	yealink						
3	CN=sanzhang,OU=yealink,DC=ldap,DC=yealink,DC=com	contact		san zhang	san zhang	san	zhang	sz	1111	123456789001
4	CN=sili,OU=yealink,DC=ldap,DC=yealink,DC=co	contact		si li	si li	li	si	sl	2222	123456789002
5	CN=wuwang,OU=yealink,DC=ldap,DC=yealink,DC=com	contact		wu wang	wu wang	wang	wu	ww	3333	123456789003

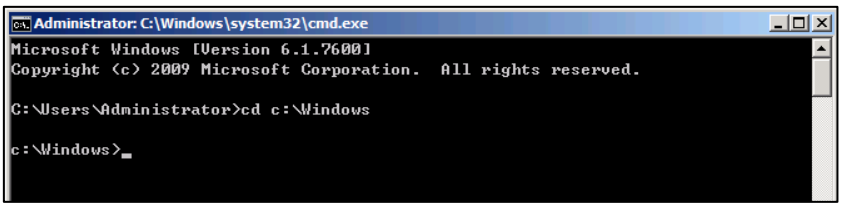
The first line lists the attributes of the entries.

The second line lists the values of an organizational unit in the corresponding attribute columns.

The other lines list the values of contacts in the corresponding attribute columns.

To import the test.csv file:

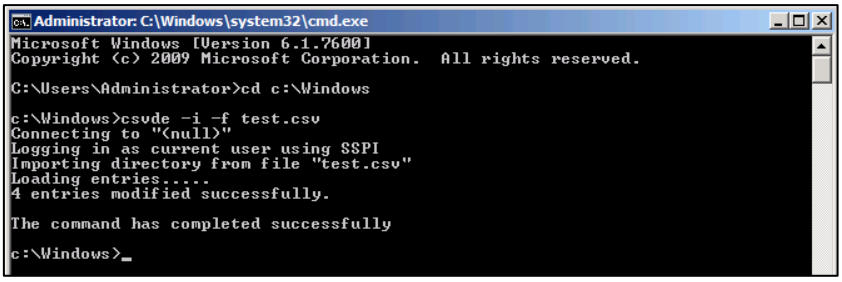
1. Click **Start**->**Run**.
2. Enter **cmd** in the pop-up dialogue box and click **OK** to enter the command line interface.
3. Execute the command **cd** to access the path of the test.csv file. For example, execute **cd c:\Windows** to access the path of the test.csv file at **c:\Windows**.



4. Execute the command **csvde -i -f test.csv** to import the file.

   If the entries are added successfully, you can find the prompt "**n entries modified successfully**" ("n" indicates the number of the added entries).

   The screenshot for reference is shown as below:



The csvde tool cannot edit or delete the existing entries on the active directory.

You can also export the existing entries on the active directory into a *.csv file first, modify the file, and then import the modified file into the active directory. For more information, refer to the network resource.

Creating User Accounts

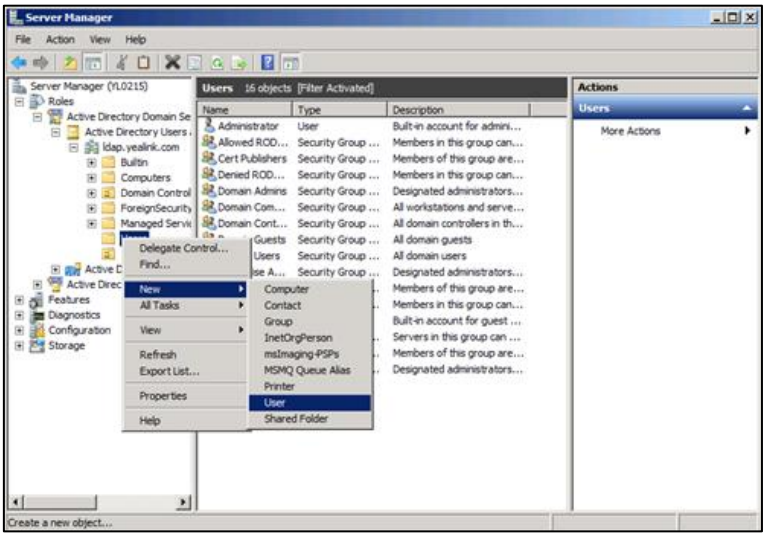
You can create user accounts to allow access to resources on the active directory. User accounts are very important and useful.

To create a user account:

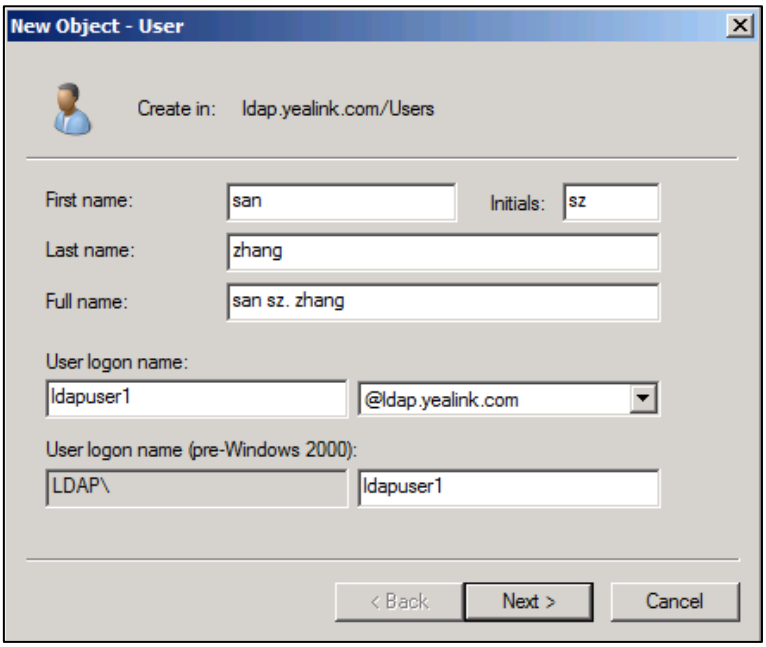
1. Click **Start**->**Administrative Tools**->**Server Manager**.
2. Double click **Server Manager**->**Roles**->**Active Directory Domain Services**->**Active**

Directory Users and Computers.

3. Select the domain name created above (e.g., ldap.yealink.com).
4. Right-click **Users**, and then select **New**->**User**.

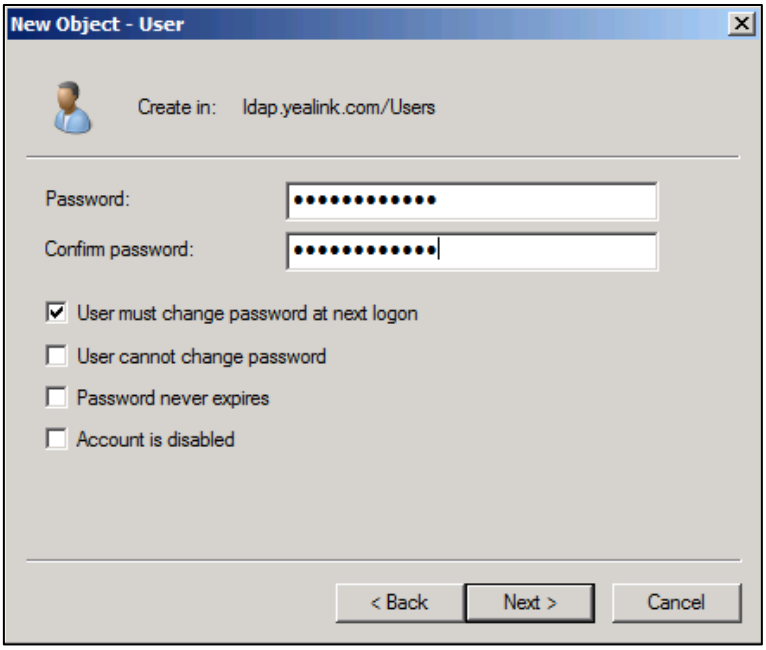


5. Enter desired values in the corresponding fields and click **Next**.

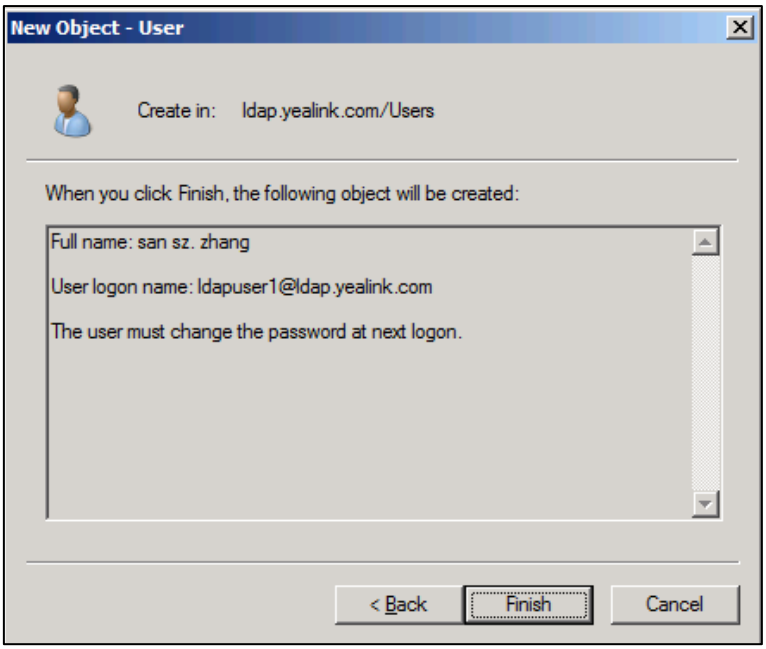


6. Enter the password for the user, select the appropriate options and click **Next**.

The password should be a combination of upper case letters, lower case letters, numbers, and special characters.



7. Click **Finish** to complete the creation of the user account.



Microsoft Active Directory Application Mode

Microsoft Active Directory Application Mode (ADAM) is a new mode of Active Directory that is designed specifically for directory-enabled applications. ADAM is a Lightweight Directory Access Protocol (LDAP) directory service that runs as a user service, rather than as a system service. You can run ADAM on servers and domain controllers running operating systems in the Windows

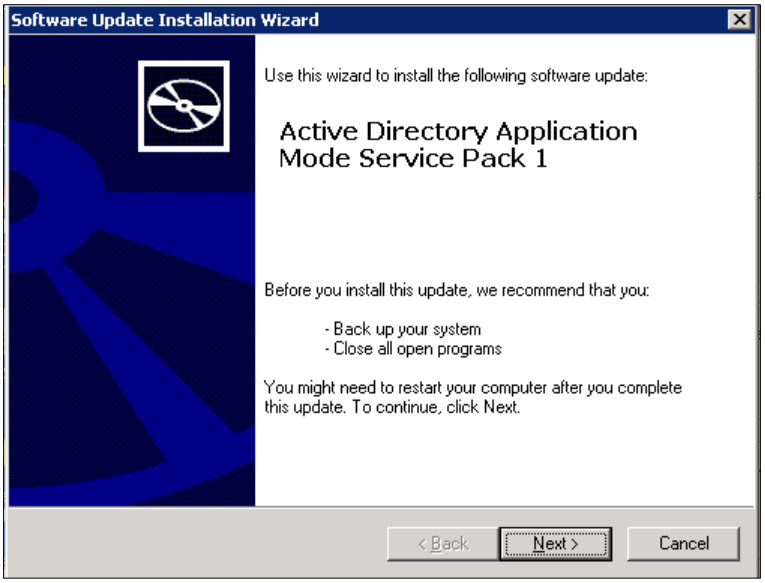
Server 2003 family. This section shows you how to install Active Directory Application Mode (ADAM) on Microsoft Windows Server 2003 SP2 Enterprise 32-bit system. You can download Active Directory Application Mode (ADAM) online:

http://www.microsoft.com/en-us/download/confirmation.aspx?id=4201.

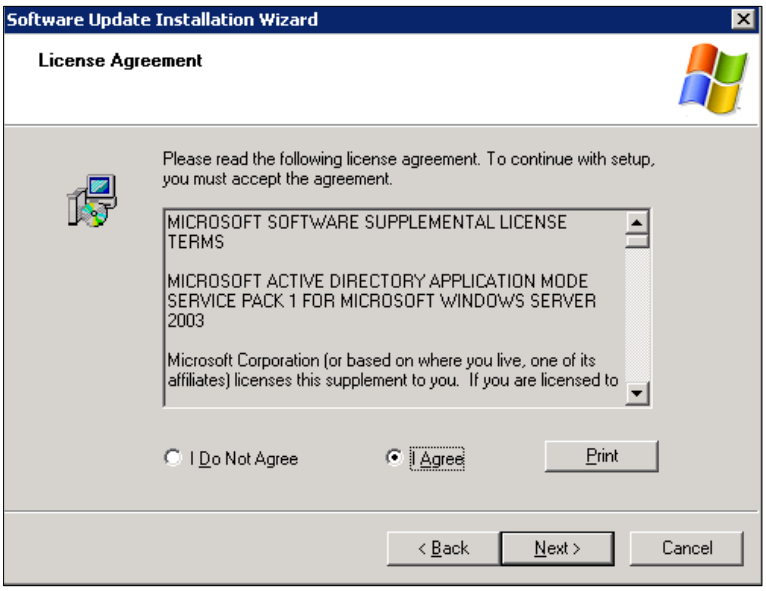
Installing the Active Directory Application Mode

To install the Active Directory Application Mode:

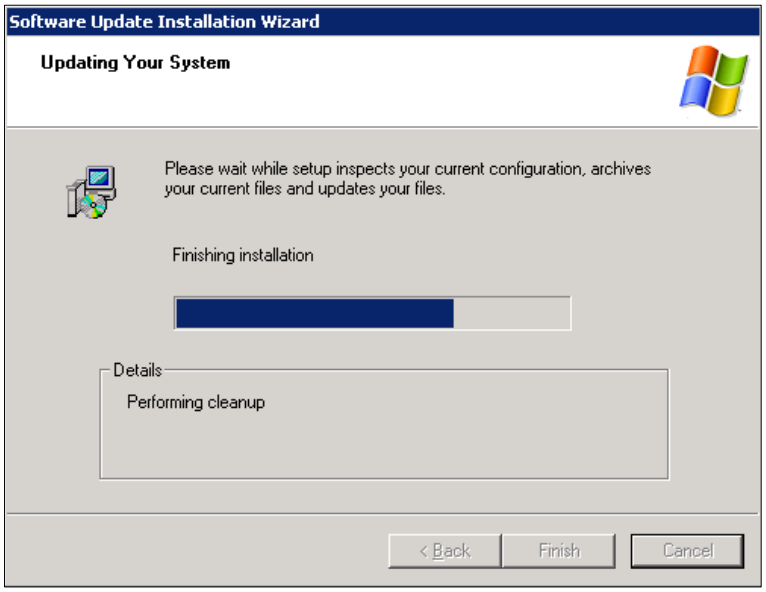
1. Double click ADAMSP1_x86_English.exe to run the application.
2. The Active Directory Application Mode Service Park 1 Installation Wizard will appear after a short while, click **Next**.



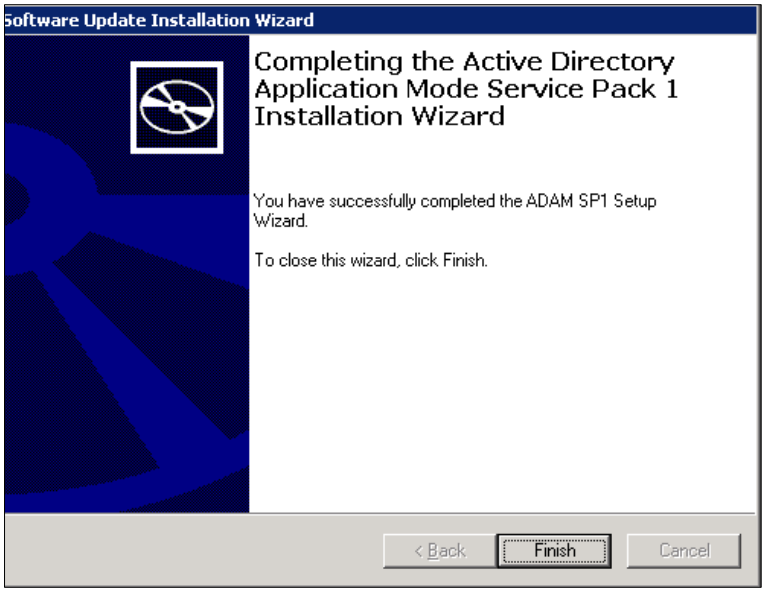
3. Read the software license agreement and mark **I Agree** radio box. And then click **Next**.



The installation progress screen will be shown as below:



4. Click **Finish** to complete the installation and exit the wizard.

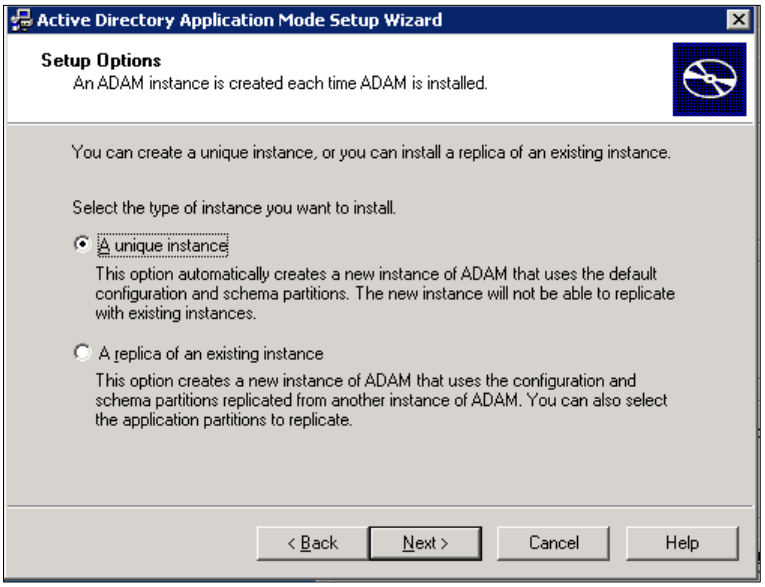


To create an ADAM instance:

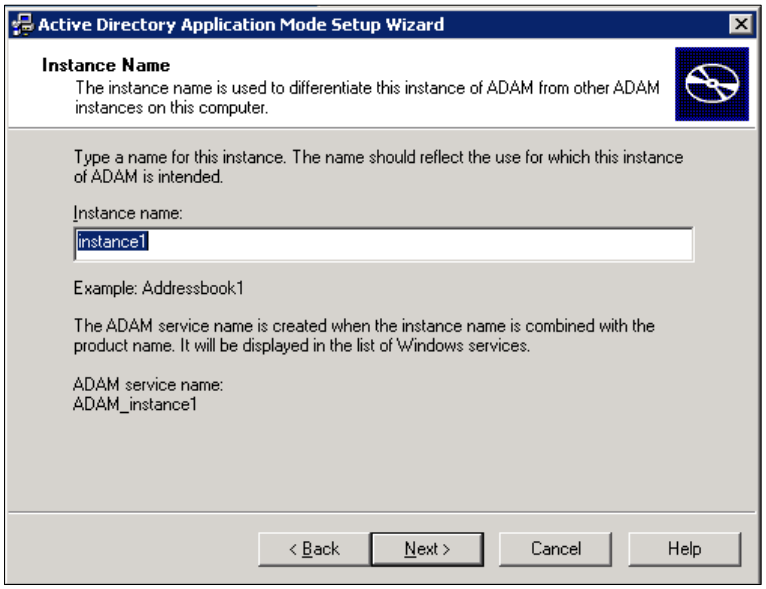
1. Click **Start**->**Programs**->**ADAM**->**Create an ADAM instance.**

   It will prompt the following interface and click **Next**.

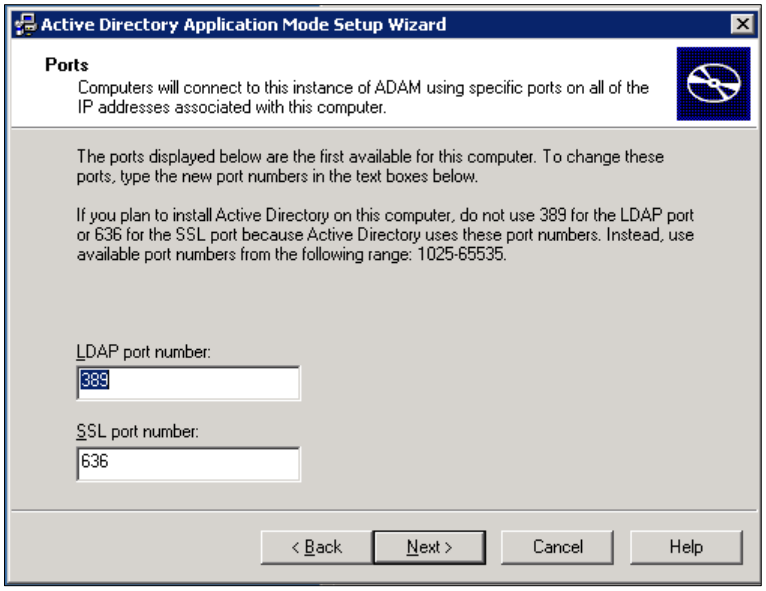
2. Mark the **A unique instance** radio box and click **Next**.



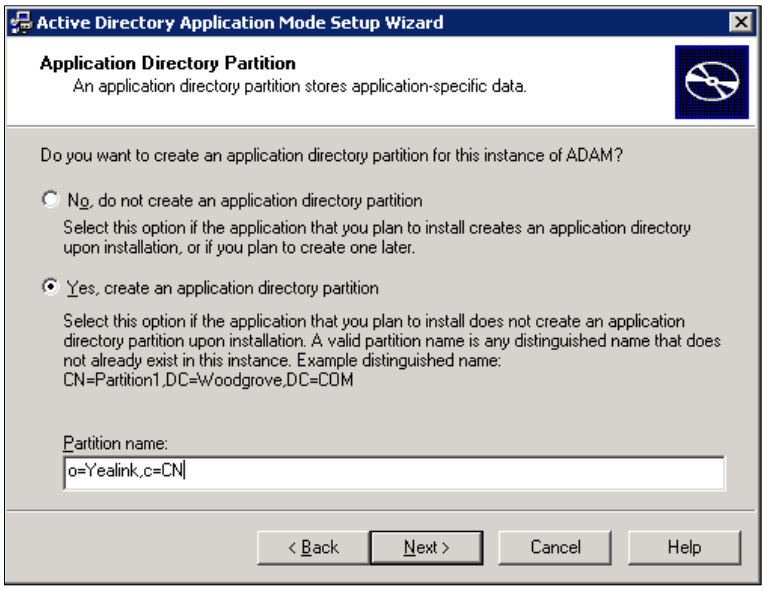
3. Enter the desired name in the **Instance name** field and click **Next**.



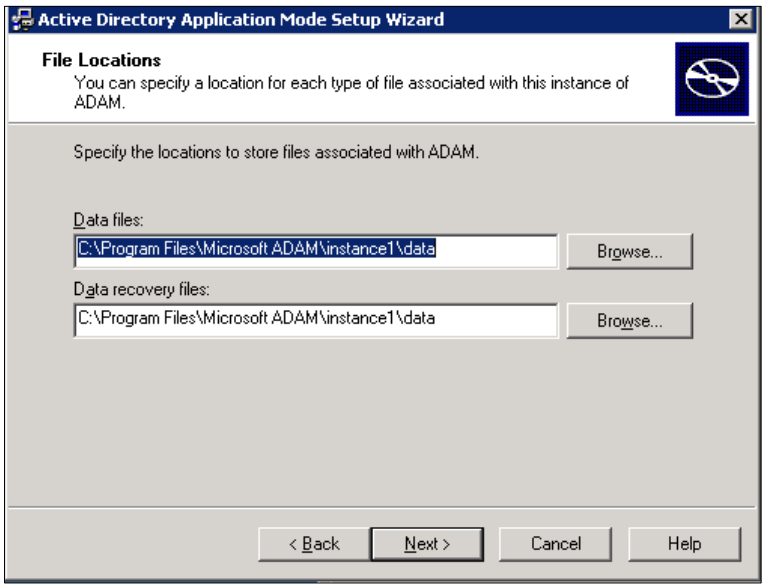
4. Keep the default ports and click **Next**.



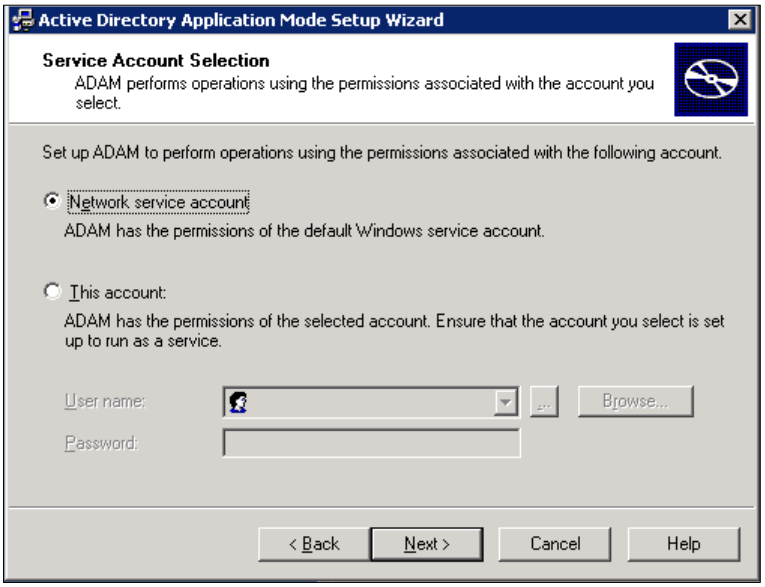
5. Mark the **Yes, create an application directory partition** radio box and enter the desired name (e.g., o=Yealink,c=CN) in the **Partition name** field, and then click **Next**.



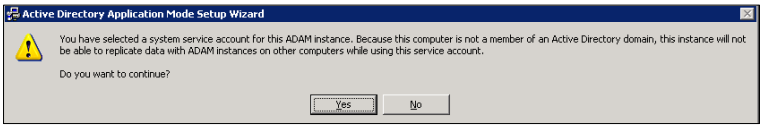
6. Specify the desired paths for the data and data recovery files, and click **Next**.



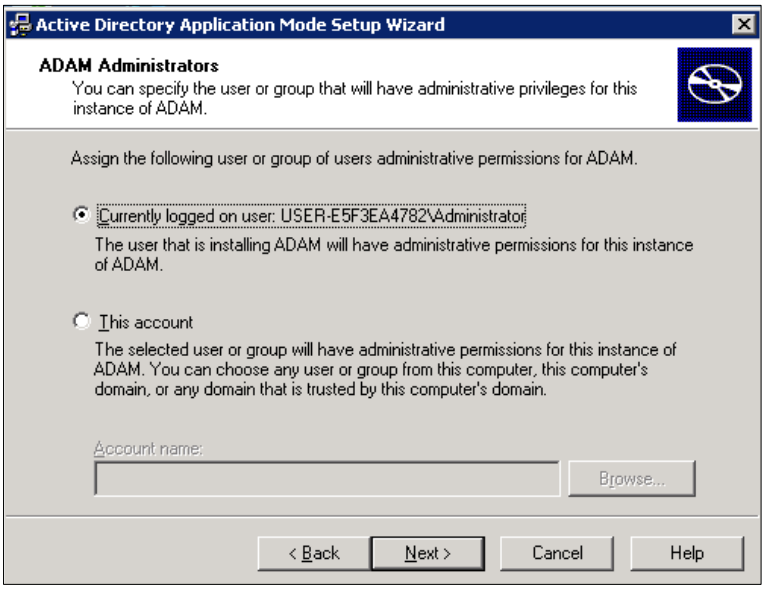
7. Mark the **Network service account** radio box and click **Next**.



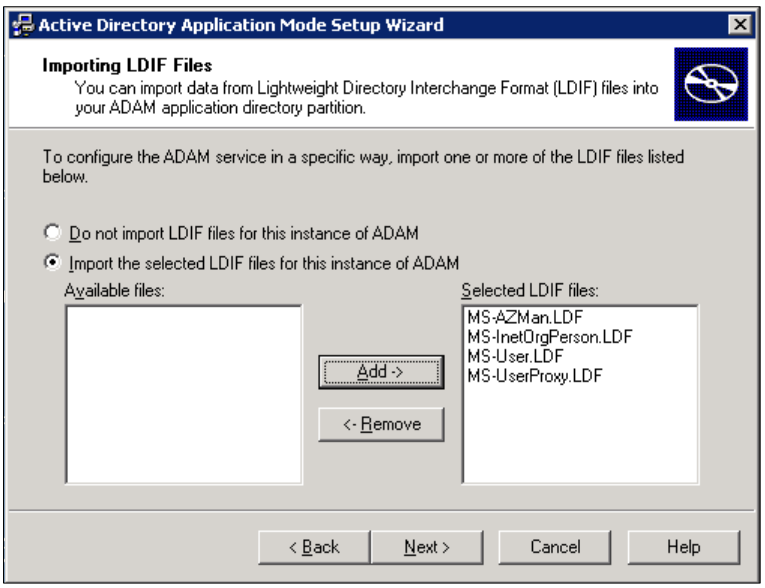
It will pop up the following prompt box. Read the provided information and click **Yes**.



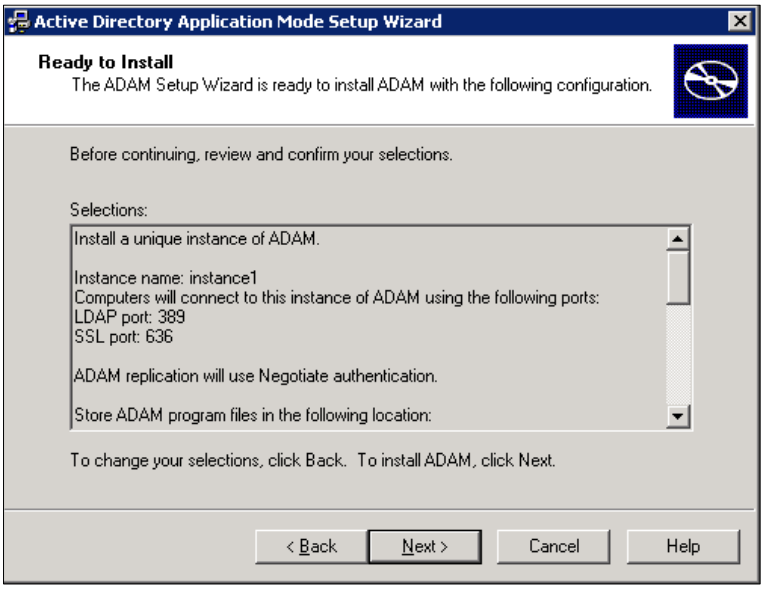
8. Mark the first radio box to assign the administrative permissions for ADAM to the currently logged on user (e.g., USER-E5F3EA4782) and click **Next**.



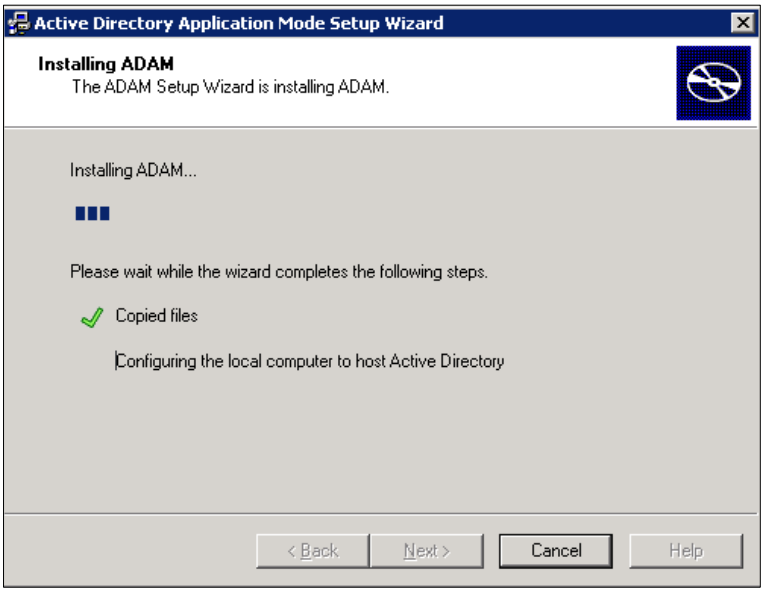
9. Mark the **Import the selected LDIF files for this instance of ADAM** radio box.
10. In the **Available files** box, select the desired LDF files and then click **Add->**, and then click **Next**.



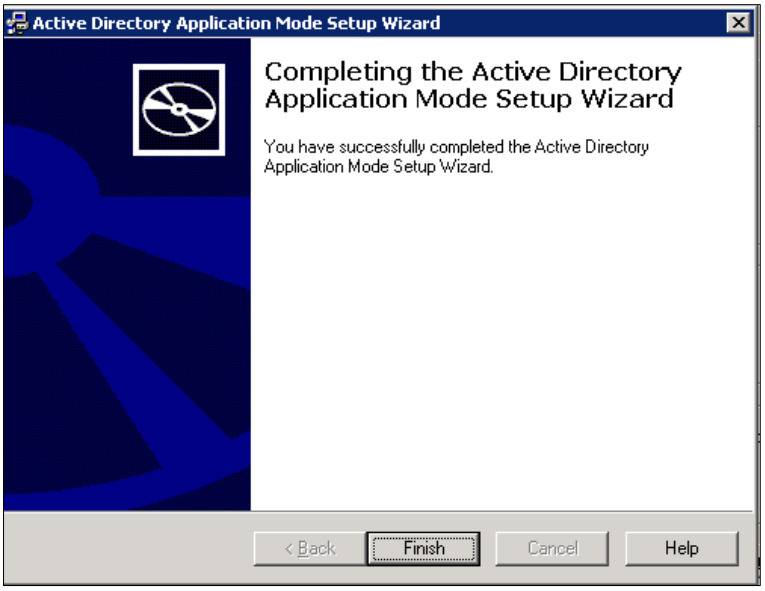
11. Review your selection and click **Next**.



The installing progress is shown as below:



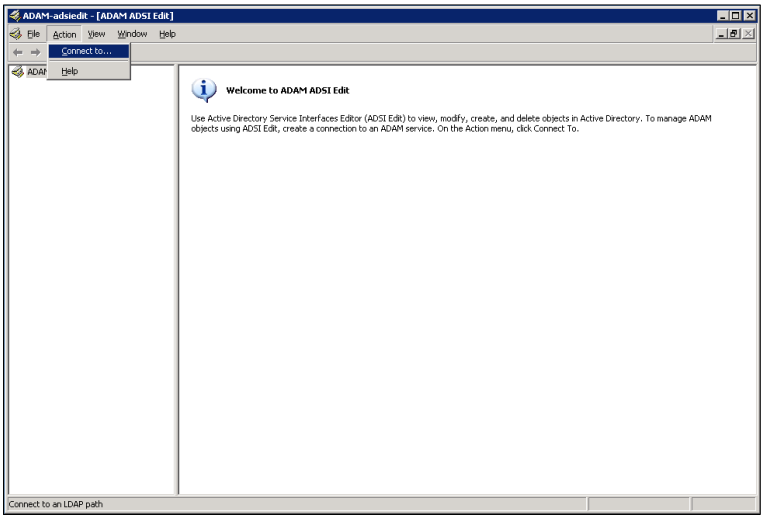
12. Click **Finish** to complete the installation and exit the wizard.



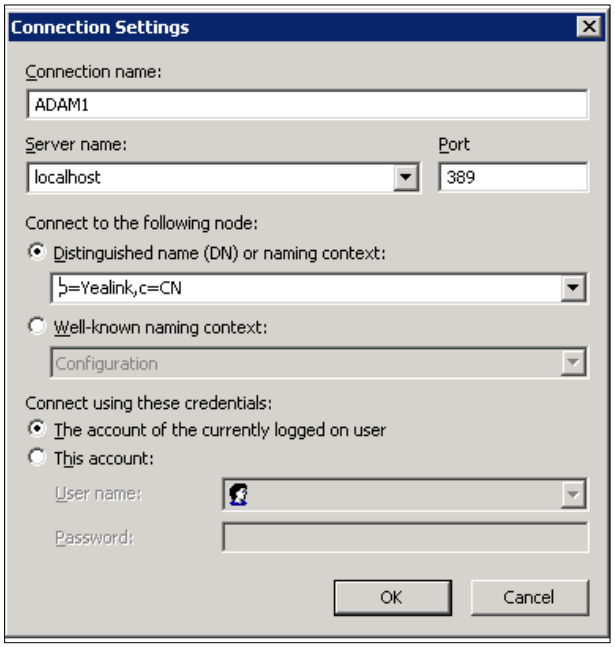
Configuring the ADAM ADSI Edit

To configure the ADAM ADSI Edit:

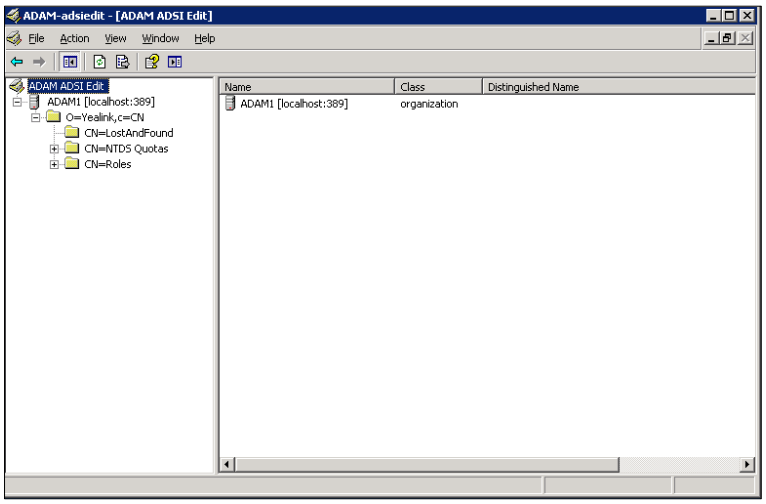
1. Click **Start**->**Programs**->**ADAM**->**ADAM ADSI Edit.**
2. Click **Action->Connect to.**



3. Enter the desired name (e.g., ADAM1) in the **Connection name** field.
4. Mark the **Distinguished name (DN) or naming context** radio box and enter the desired value (e.g., o=Yealink,c=CN) in the following field.
5. Click **OK**.

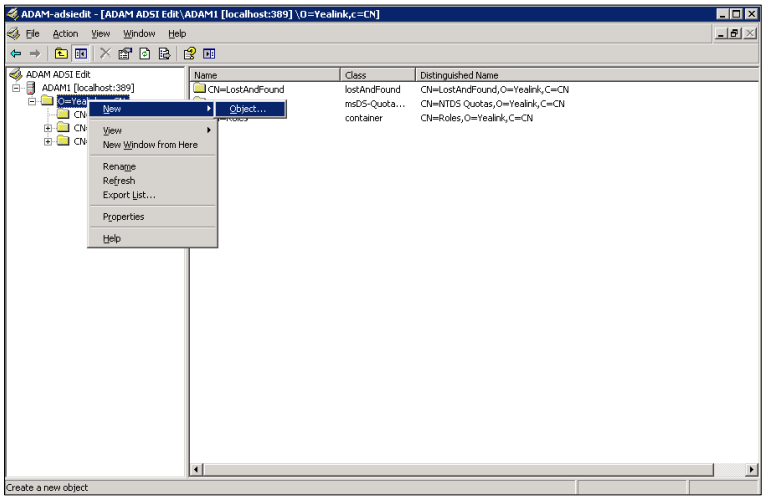


When the ADAM ADSI Edit connects an application directory partition (e.g., o=Yealink,c=CN) successfully, it will show as below:

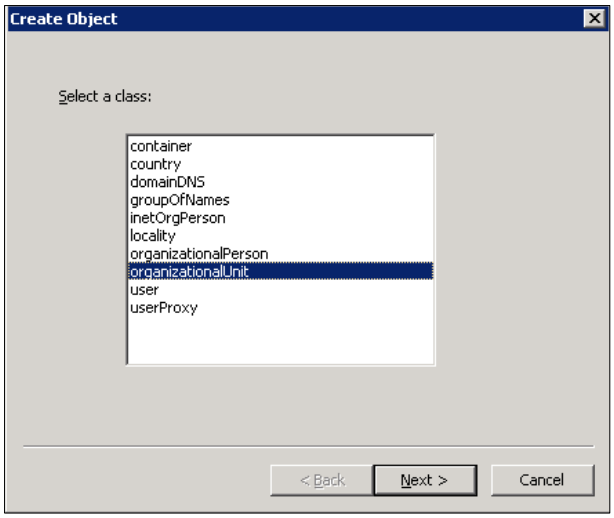


To create the object for ADAM:

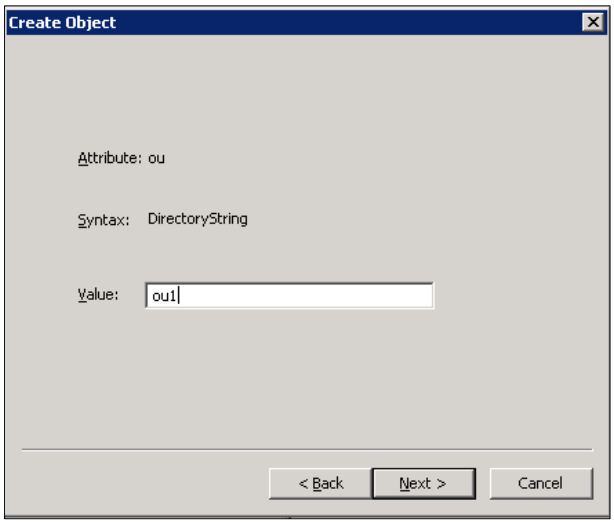
1. Select and right-click **O=Yealink,c=CN**, and then select **New**->**Object**.



2. Select **organizationalUnit** and click **Next**.

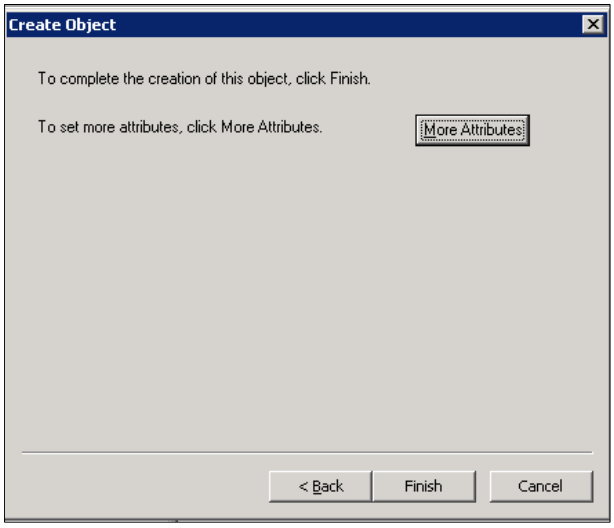


3. Enter the desired value (e.g., ou1) in the **Value** field and click **Next**.

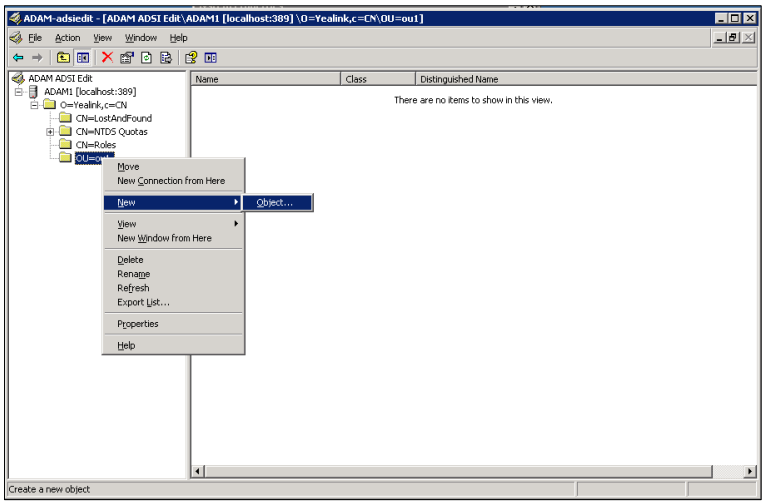


4. Click **Finish** to complete the creation of this object.

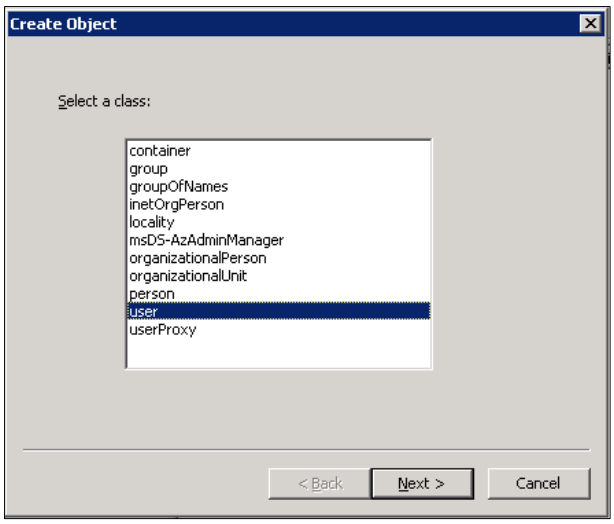
You can also click **More Attributes** to set more attributes for this object.



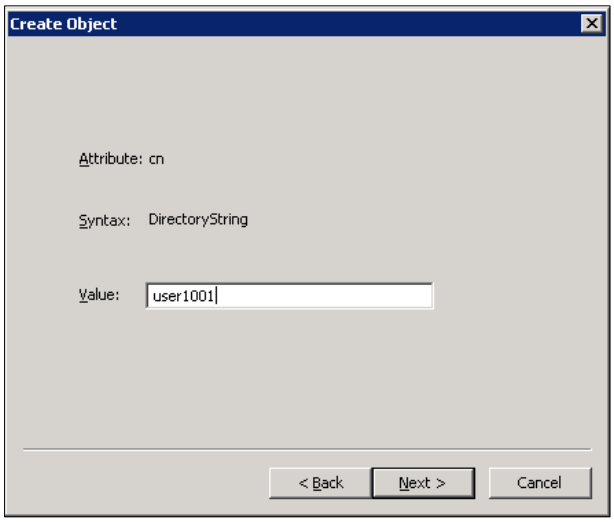
5. Select and right-click **OU=ou1**, and then select **New**->**Object**.



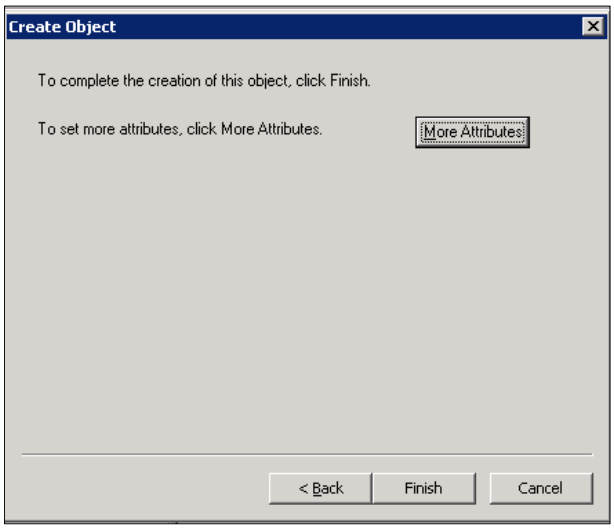
6. Select **user** and click **Next**.



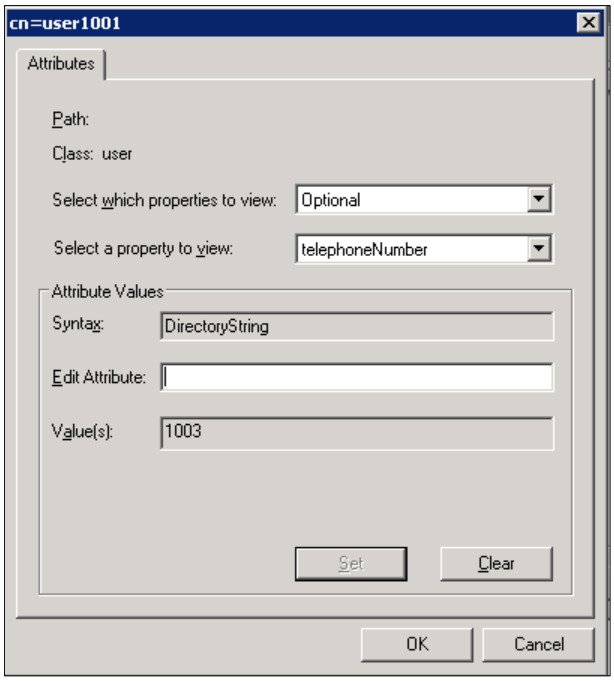
7. Enter the desired value (e.g., user1001) in the **Value** field and click **Next**.



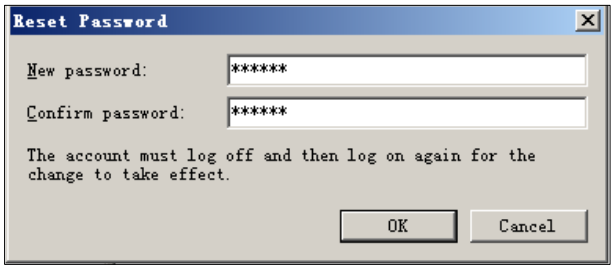
8. Click **More Attributes** to set more attributes for this user.



9. In the popup dialog of Attributes, select the **telephoneNumber** from the **Select a property to view** drop-down menu. Enter the desired telephone number (e.g., 1003) in the **Edit Attribute** field and click **Set**. The entered telephone number will be shown in the **Value(s)** field.



10. Click **OK** to close the Attributes dialog, and click **Finish** to complete the creation of this user.
11. Select and right-click the user created above, and then select **Reset Password**.
12. Enter the password for the user created above in the **New password** field and **Confirm password** field respectively.

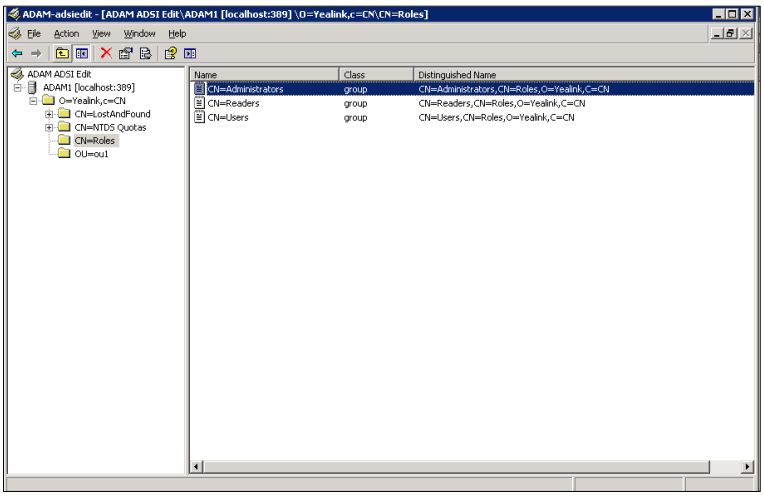


13. Click **OK** to accept the change.

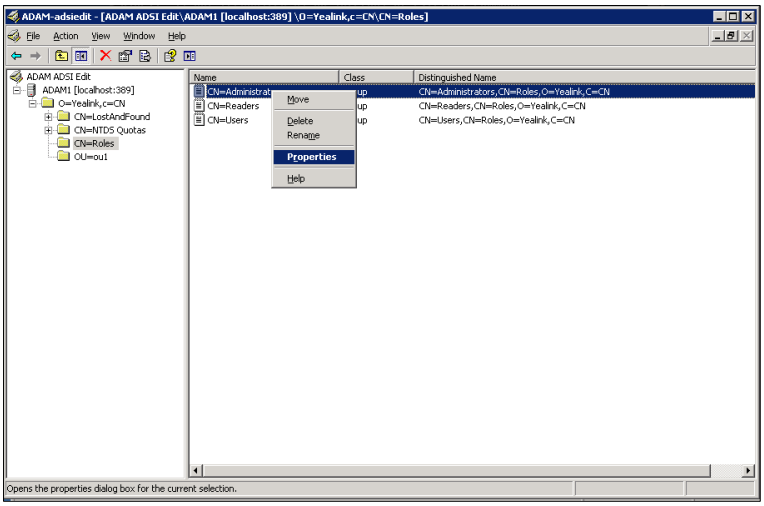
If you want to use the user created above to manage and search for information of LDAP, you need to add the user to the administrator group in advance.

To add the user to the administrator group:

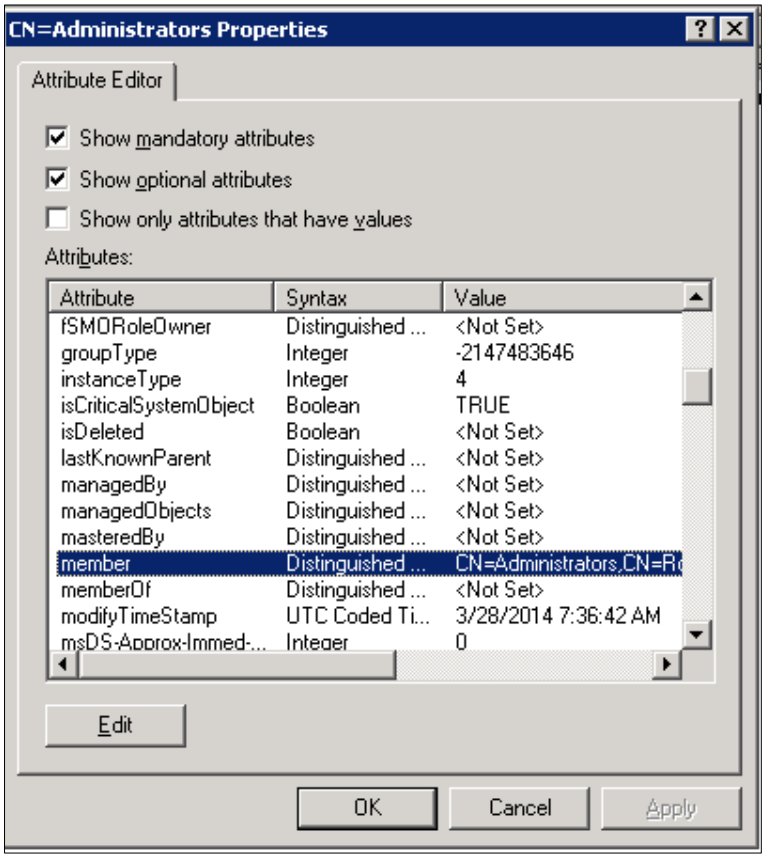
1. Click **ADAM1**->**O=Yealink, c=CN**->**CN=Roles.**



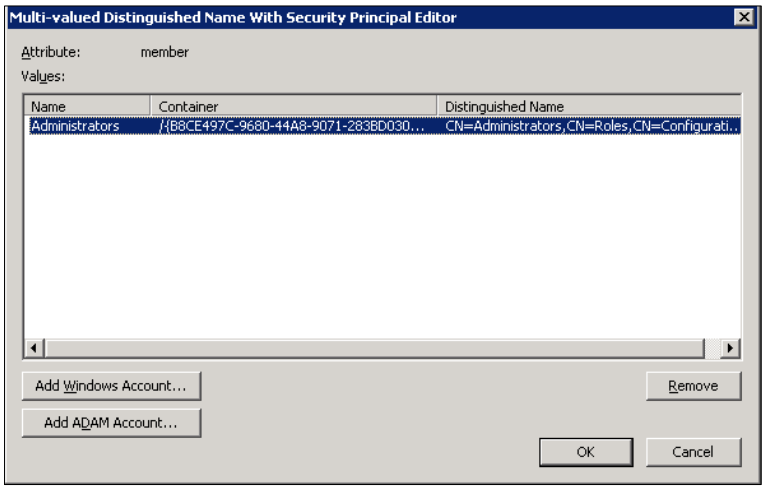
2. Select and right-click **CN=Administrators,** and then select **Properties.**



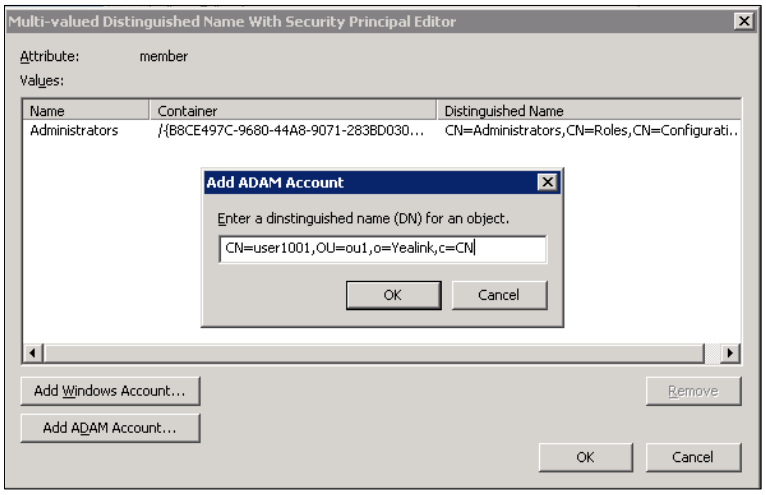
3. Select the **member** attribute in the **Attributes** box and click **Edit**.



4. In the popup dialog of the member attribute, click **Add ADAM Account**.



5. In the popup dialog of adding the ADAM account, enter the desired distinguished name (e.g., CN=user1001,OU=ou1,o=Yealink,c=CN) in the field.

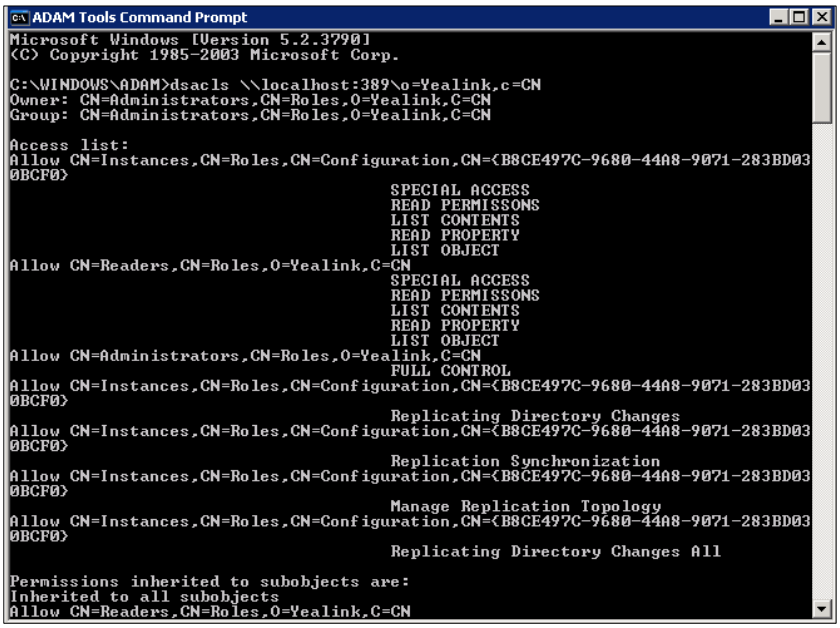


6. Click **OK** to accept the change and close the dialog of adding the ADAM account.
7. Click **OK** to accept the change and close the dialog of the member attribute.
8. Click **OK** to accept the change and close the Administrators Properties interface.

You can also view the permissions of ADAM using the command.

To view permissions using the command:

1. Click **Start**->**Programs**->**ADAM**->**ADAM Tools Command Prompt.**
2. Execute the command **dsacls \\localhost:389\o=Yealink,c=CN** view permissions of o=Yealink,c=CN.



```
ADAM Tools Command Prompt
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\WINDOWS\ADAM>dsacls \\localhost:389\o=Yealink,c=CN
Owner: CN=Administrators,CN=Roles,O=Yealink,C=CN
Group: CN=Administrators,CN=Roles,O=Yealink,C=CN

Access list:
Allow CN=Instances,CN=Roles,CN=Configuration,CN={B8CE497C-9680-44A8-9071-283BD03
0BCF0}
                                        SPECIAL ACCESS
                                        READ PERMISSONS
                                        LIST CONTENTS
                                        READ PROPERTY
                                        LIST OBJECT
Allow CN=Readers,CN=Roles,O=Yealink,C=CN
                                        SPECIAL ACCESS
                                        READ PERMISSONS
                                        LIST CONTENTS
                                        READ PROPERTY
                                        LIST OBJECT
Allow CN=Administrators,CN=Roles,O=Yealink,C=CN
                                        FULL CONTROL
Allow CN=Instances,CN=Roles,CN=Configuration,CN={B8CE497C-9680-44A8-9071-283BD03
0BCF0}
                                        Replicating Directory Changes
Allow CN=Instances,CN=Roles,CN=Configuration,CN={B8CE497C-9680-44A8-9071-283BD03
0BCF0}
                                        Replication Synchronization
Allow CN=Instances,CN=Roles,CN=Configuration,CN={B8CE497C-9680-44A8-9071-283BD03
0BCF0}
                                        Manage Replication Topology
Allow CN=Instances,CN=Roles,CN=Configuration,CN={B8CE497C-9680-44A8-9071-283BD03
0BCF0}
                                        Replicating Directory Changes All

Permissions inherited to subobjects are:
Inherited to all subobjects
Allow CN=Readers,CN=Roles,O=Yealink,C=CN
```

Sun One Directory Server

Sun One Directory Server, also known as Sun Java System Directory Server, is a component of the Java Enterprise System. Sun One Directory Server can be installed on multiple platforms, such as Windows, Linux, Solaris and so on. This section shows you how to install Sun One Directory Server version 5.2 on Microsoft Windows Server 2003 SP2 Enterprise 32-bit system. You can download it online: http://download.csdn.net/download/wbsoso/6439291.

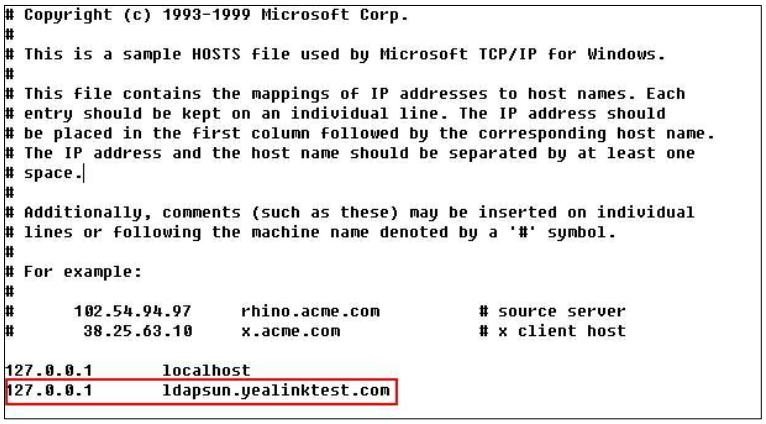
Before the installation, you should prepare as follows:

- Modify the hosts file of your computer.
- Install the Java Development Kit (JDK) 5 or later.

To modify the hosts file of your computer:

1. Locate the hosts file in the path "C:\WINDOWS\system32\drivers\etc\hosts".
2. Open and edit the hosts.dz file using your favorite text editor.
3. Add FQCN (Fully Qualified Computer Name) of your computer to the file. For example, the FQCN of your computer is ldapsun.yealinktest.com. Add the following mapping:

   127.0.0.1 ldapsun.yealinktest.com



```
# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

127.0.0.1       localhost
127.0.0.1       ldapsun.yealinktest.com
```

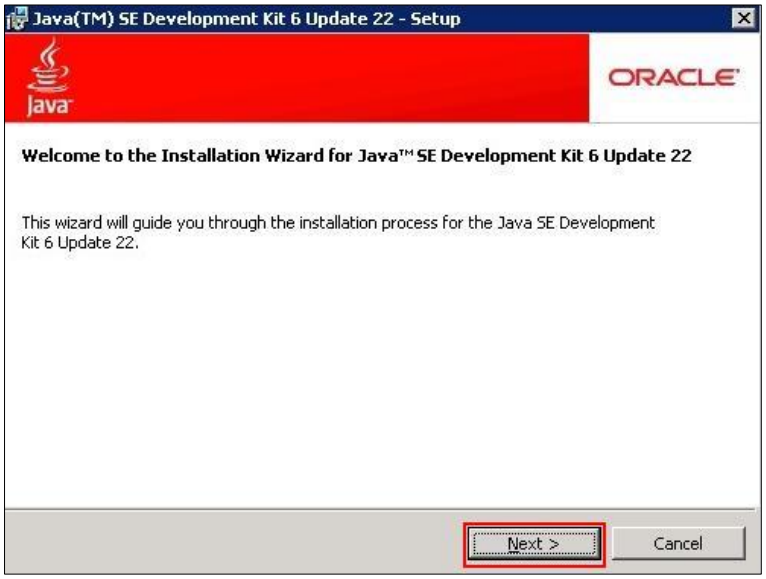
4. Save the hosts file.

The following shows you how to install the Java Development Kit (JDK) 6 on your computer. You can download it online: http://www.oracle.com/technetwork/java/javase/downloads/index.html.

To install the Java Development Kit (JDK) 6:

1. Double click jdk-6u22-windows-i586.exe to run the application.

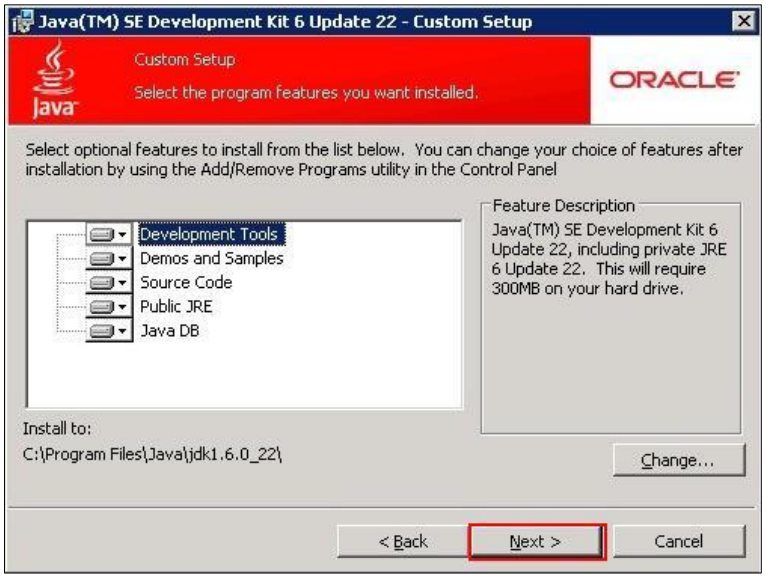
2. The Java (TM) SE Development Kit 6 Update 22 Installation Wizard will appear after a short while, click **Next**.

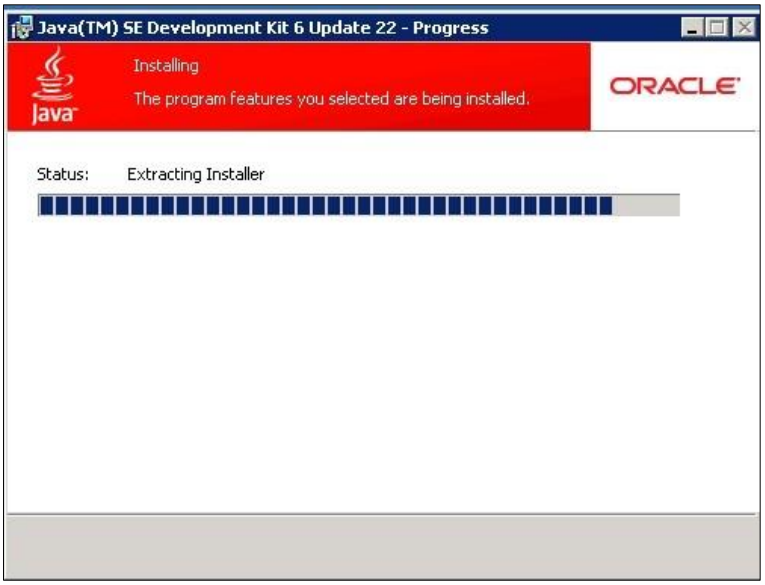


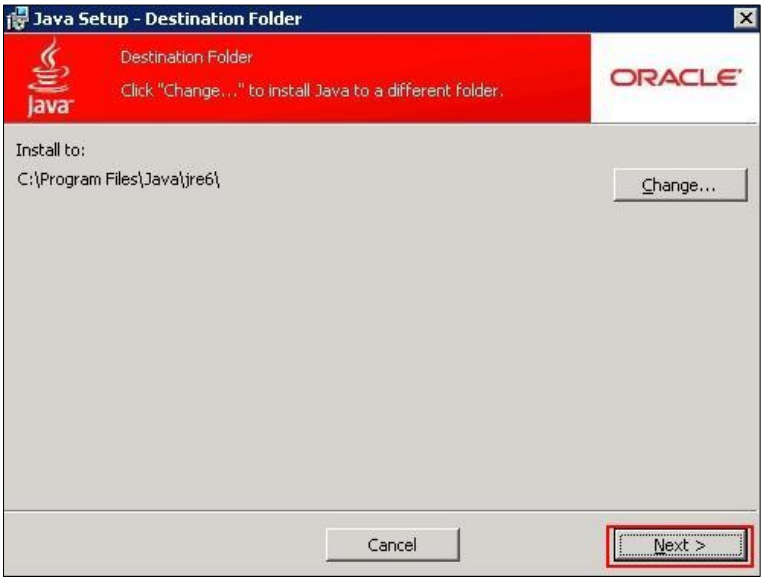
3. Click **Change** to locate the installation path from the local computer system and then click **Next**.

You need to remember the installation path (e.g., C:\Program Files\Java\jdk1.6.0_22) located here.

The screenshot for reference is shown as below:




Java(TM) SE Development Kit 6 Update 22 - Progress
Installing
The program features you selected are being installed.
ORACLE
Status: Extracting Installer


Java Setup - Destination Folder
Destination Folder
Click "Change..." to install Java to a different folder.
ORACLE
Install to:
C:\Program Files\Java\jre6\
Change...
Cancel
Next >

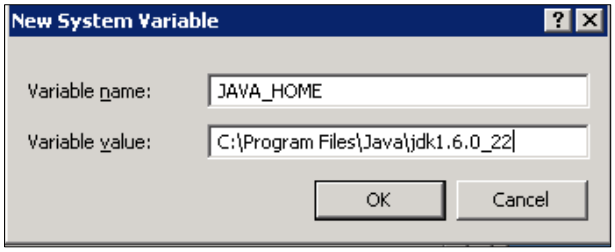
Java Setup - Progress
Installing Java
This may take a few minutes
ORACLE
Status: Extracting Installer
Now you can have a full-featured office suite that's compatible with Microsoft Office for free!
Powerful, integrated set of word processing, spreadsheet, presentation, drawing and database applications
Reads, edits and saves Microsoft Office files
Supports over 70 languages and Solaris, Windows, Linux and Mac operating systems
Uses industry-standard, open file format (OpenDocument) as its default file format
Built-in, one-click PDF export
Writer
Calc
Impress
Base
Draw
Math
OpenOffice.org

4. Click **Finish** to finish the installation.

After the installation, you need to configure environment variables.

To configure environment variables:

1. Right-click the **My Computer** icon and select **Properties**.
2. Click the **Advanced** tab.
3. Click the **Environment Variables** button.
4. Add the following variables, click **New** under **System Variables**.
5. Enter the variable name as JAVA_HOME.
6. Enter the variable value as the installation path (e.g., C:\Program Files\Java\jdk1.6.0_22) for the Java Development Kit.



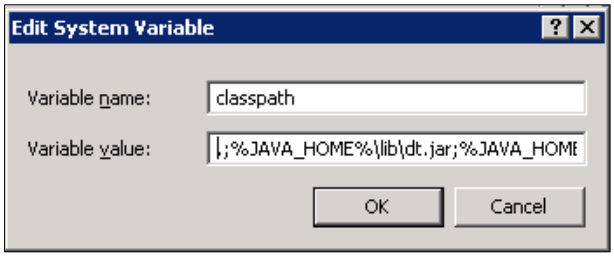
7. Click **OK**.
8. Repeat steps 4-7 to create a new system variable.

   Variable name: classpath

   Variable value: .;%JAVA_HOME%\lib\dt.jar;%JAVA_HOME%\lib\tools.jar

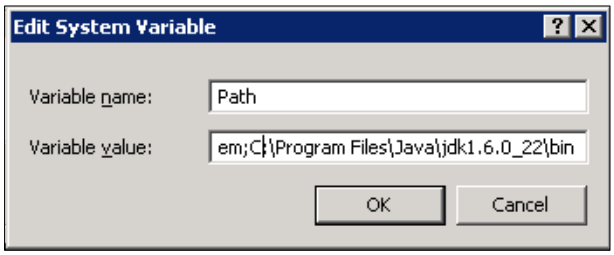
   The dot "." stands for the current path and it can't be deleted.

%JAVA_HOME% references the value of the specified JAVA_HOME variable created before.



9. Under **System Variables**, select the **Path** variable and click **Edit**.
10. In the **Variable value** field, append the Java bin directory (e.g., C:\Program Files\Java\jdk1.6.0_22\bin) to the end of the existing path (e.g., %SystemRoot%\system32;%SystemRoot%;%SystemRoot%\System32\Wbem;).

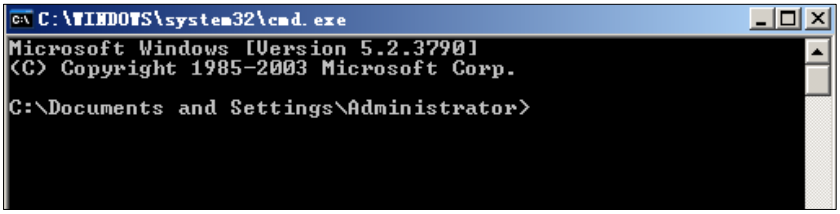
    If the end of the existing path has no semicolon, you should add a semicolon to the end of the existing path and then append the Java bin directory.



11. Click **OK**.
12. Click **Apply Changes**.

To verify the configuration of environment variables:

1. Click **Start**->**Run**.
2. Enter **cmd** in the pop-up dialogue box and click **OK** to enter the command line interface.



3. Execute the command **java -version** to check the java version.

It prompts the following information.

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>java -version
java version "1.6.0_22"
Java(TM) SE Runtime Environment (build 1.6.0_22-b04)
Java HotSpot(TM) Client VM (build 17.1-b03, mixed mode, sharing)

C:\Documents and Settings\Administrator>
```

4. Execute the command **java** to run the application.

It prompts the following information.

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>java
Usage: java [-options] class [args...]
           (to execute a class)
   or  java [-options] -jar jarfile [args...]
           (to execute a jar file)

where options include:
    -client       to select the "client" VM
    -server       to select the "server" VM
    -hotspot      is a synonym for the "client" VM  [deprecated]
                  The default VM is client.

    -cp <class search path of directories and zip/jar files>
    -classpath <class search path of directories and zip/jar files>
                  A ; separated list of directories, JAR archives,
                  and ZIP archives to search for class files.
    -D<name>=<value>
                  set a system property
    -verbose[:class|gc|jni]
                  enable verbose output
    -version      print product version and exit
    -version:<value>
                  require the specified version to run
    -showversion  print product version and continue
    -jre-restrict-search | -jre-no-restrict-search
                  include/exclude user private JREs in the version sea
    -? -help      print this help message
    -X            print help on non-standard options
    -ea[:<packagename>...|:<classname>]
    -enableassertions[:<packagename>...|:<classname>]
                  enable assertions
    -da[:<packagename>...|:<classname>]
    -disableassertions[:<packagename>...|:<classname>]
```

5. Execute the command **javac** to compile java files into class files.

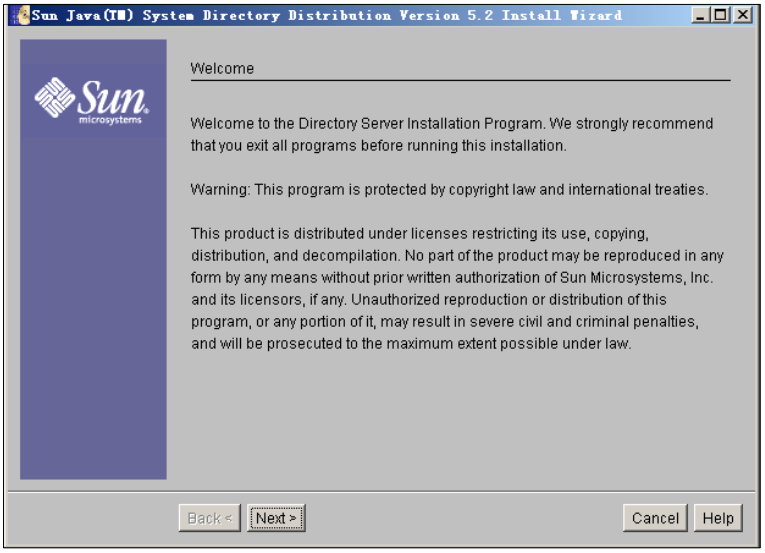
It prompts the following information.

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>javac
Usage: javac <options> <source files>
where possible options include:
  -g                         Generate all debugging info
  -g:none                    Generate no debugging info
  -g:{lines,vars,source}     Generate only some debugging info
  -nowarn                    Generate no warnings
  -verbose                   Output messages about what the compiler is doing
  -deprecation               Output source locations where deprecated APIs are
sed
  -classpath <path>          Specify where to find user class files and annota
on processors
  -cp <path>                 Specify where to find user class files and annota
on processors
  -sourcepath <path>         Specify where to find input source files
  -bootclasspath <path>      Override location of bootstrap class files
  -extdirs <dirs>            Override location of installed extensions
  -endorseddirs <dirs>       Override location of endorsed standards path
  -proc:{none,only}          Control whether annotation processing and/or comp
ation is done.
  -processor <class1>[,<class2>,<class3>...]Names of the annotation processors
o run; bypasses default discovery process
  -processorpath <path>      Specify where to find annotation processors
  -d <directory>             Specify where to place generated class files
  -s <directory>             Specify where to place generated source files
  -implicit:{none,class}     Specify whether or not to generate class files fo
implicitly referenced files
  -encoding <encoding>       Specify character encoding used by source files
  -source <release>          Provide source compatibility with specified relea

  -target <release>          Generate class files for specific VM version
  -version                   Version information
  -help                      Print a synopsis of standard options
  -Akey[=value]              Options to pass to annotation processors
  -X                         Print a synopsis of nonstandard options
  -J<flag>                   Pass <flag> directly to the runtime system

C:\Documents and Settings\Administrator>_
```

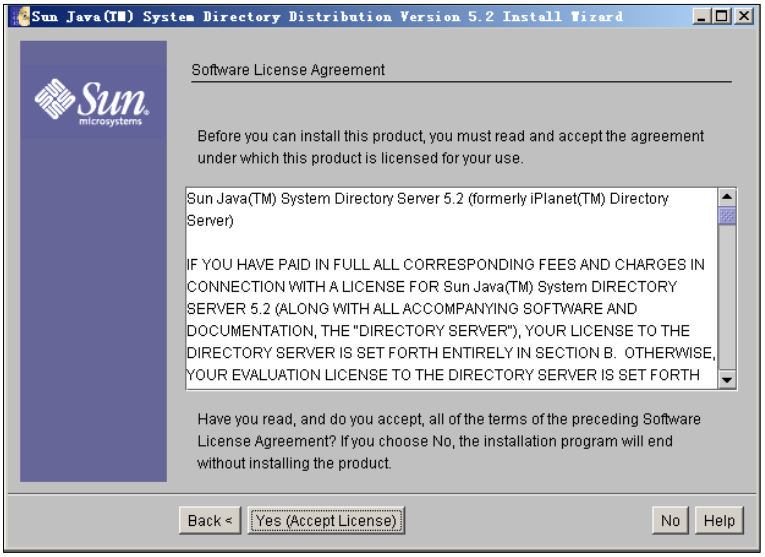
Installing the Sun One Directory

To install the Sun One Directory:

1. Unpack the compressed files named Sun Java System Directory Server.5.2.P4.Windows.full.rar.
2. Double click setup.exe to run the application.
3. The Sun Java(TM) System Directory Distribution Version 5.2 Install Wizard will appear after a short while, click **Next**.

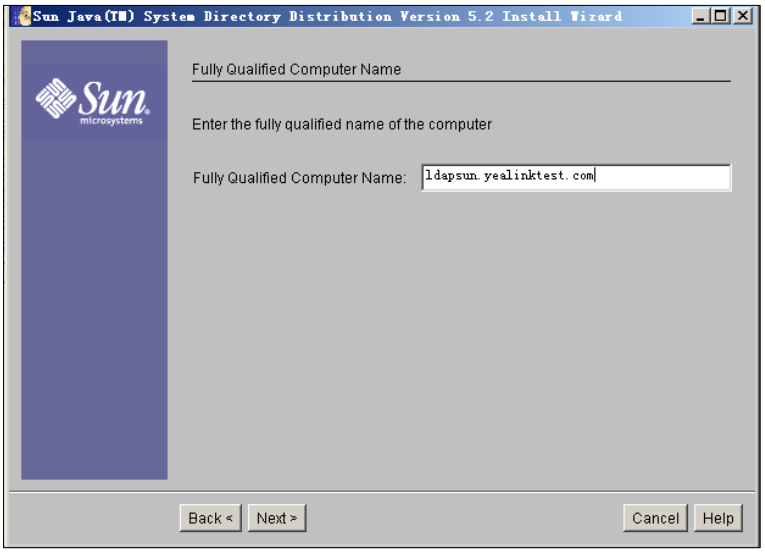


4. Read the software license agreement and click **Yes (Accept License)**.

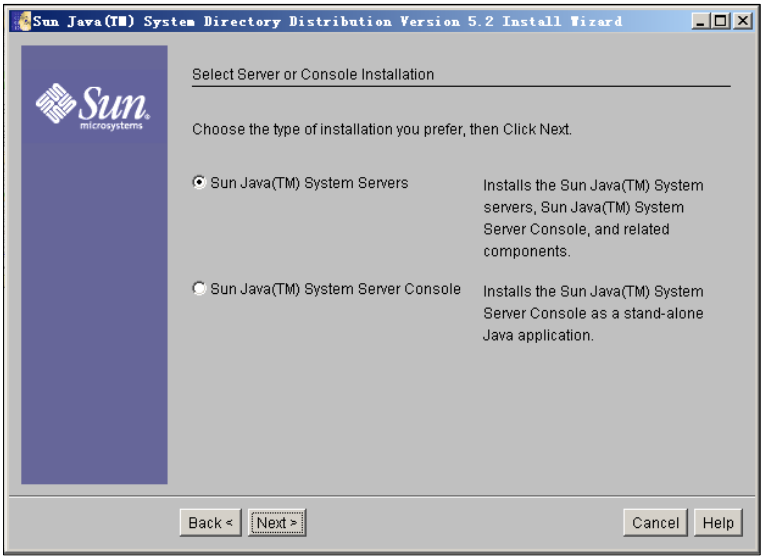


5. Enter the fully qualified name of the computer (e.g., ldapsun.yealinktest.com) in the **Fully Qualified Computer Name** field and click **Next**.

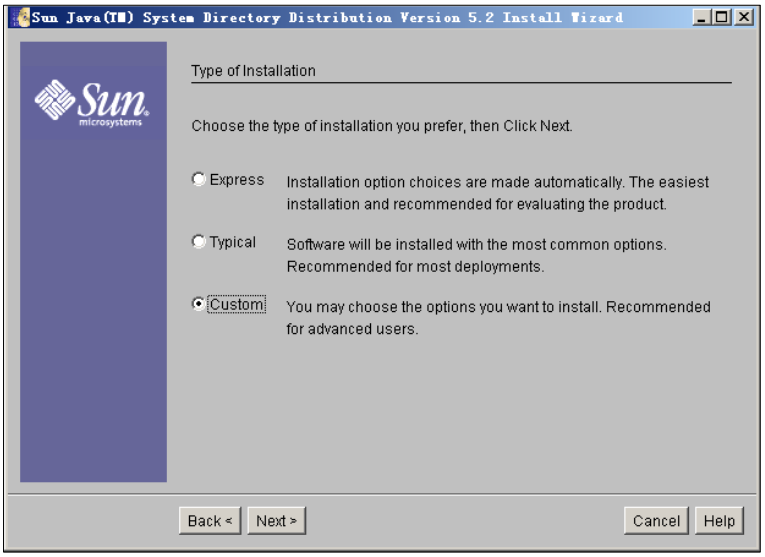
   The fully qualified name of the computer was planned before. For more information, refer to modify the hosts file of your computer.



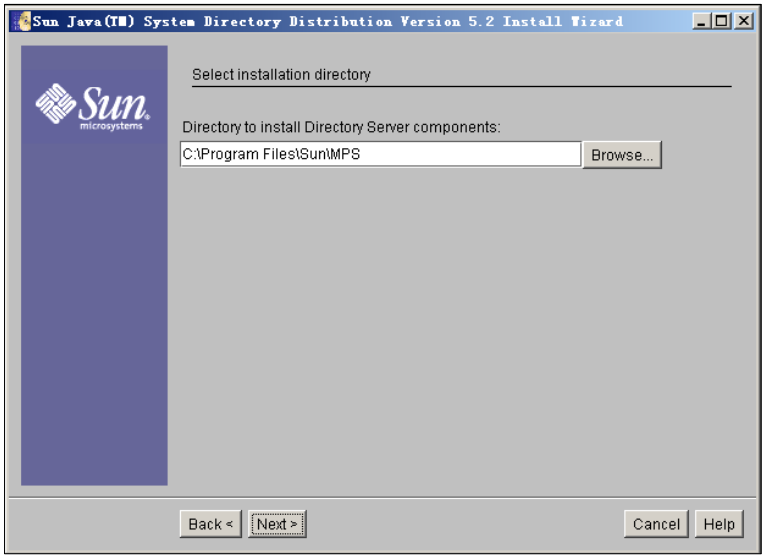
6. Mark the **Sun Java (TM) System Servers** radio box and click **Next**.



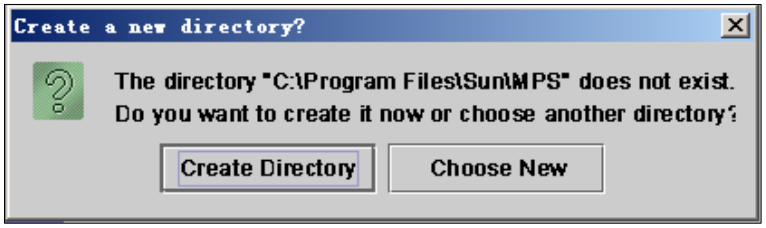
7. Mark the **Custom** radio box and click **Next**.



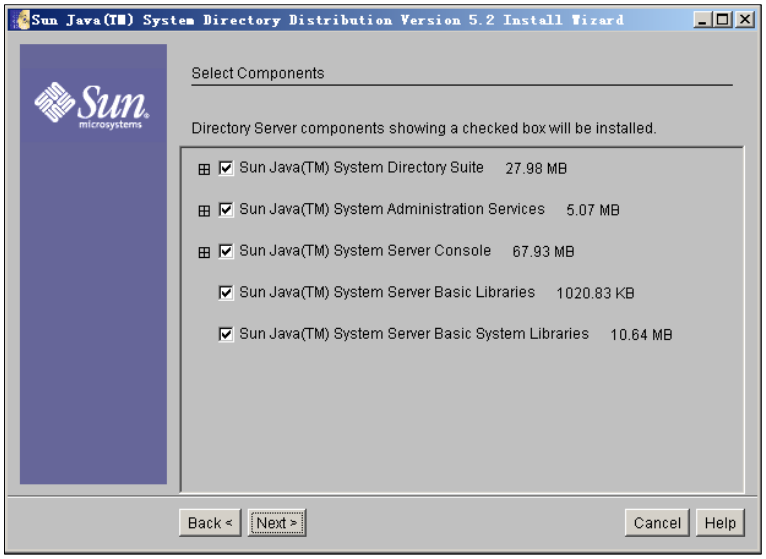
8. Specify the desired installation directory and click **Next**.



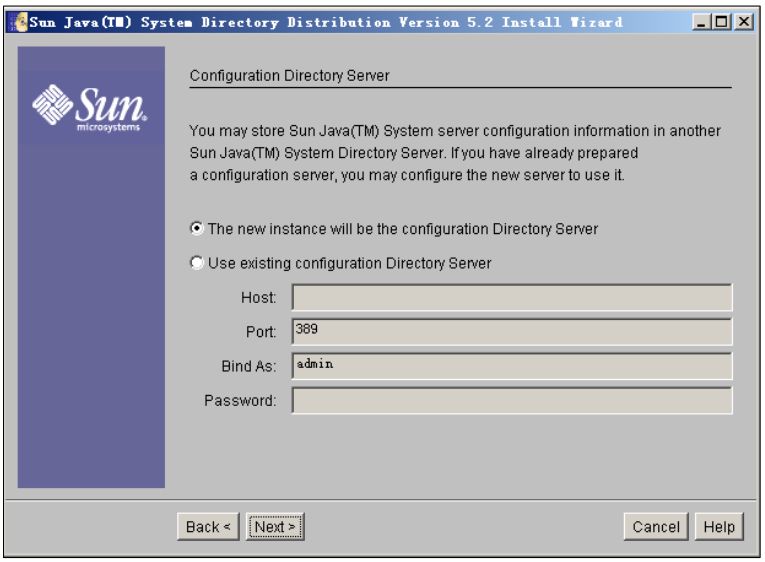
It prompts the following window. And you can click **Create Directory** to create the directory or click **Choose New** to select another path.



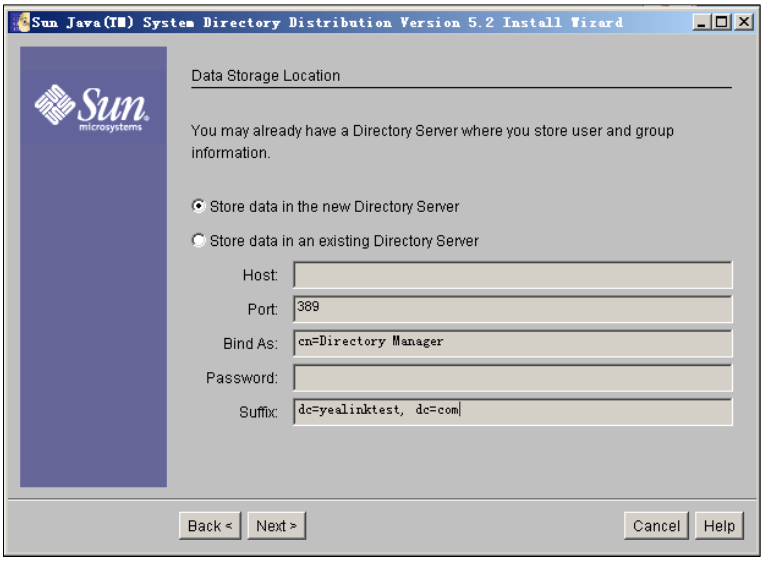
9. Select the desired installation components and click **Next**.



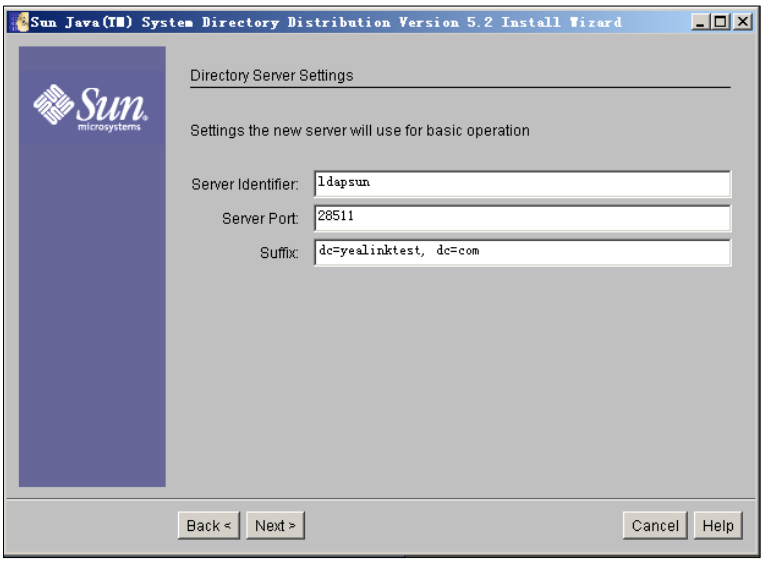
10. Mark **The new instance will be the configuration Directory Server** radio box and click **Next**.



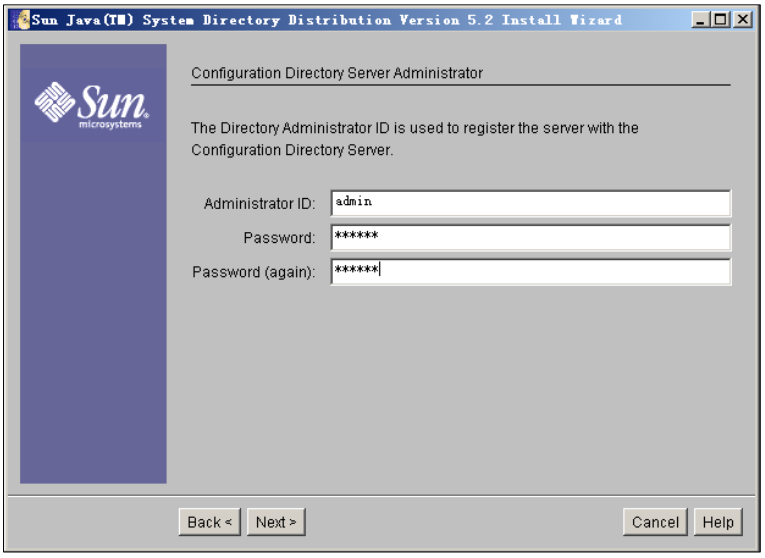
11. Mark the **Store data in the new Directory Server** radio box and click **Next**.



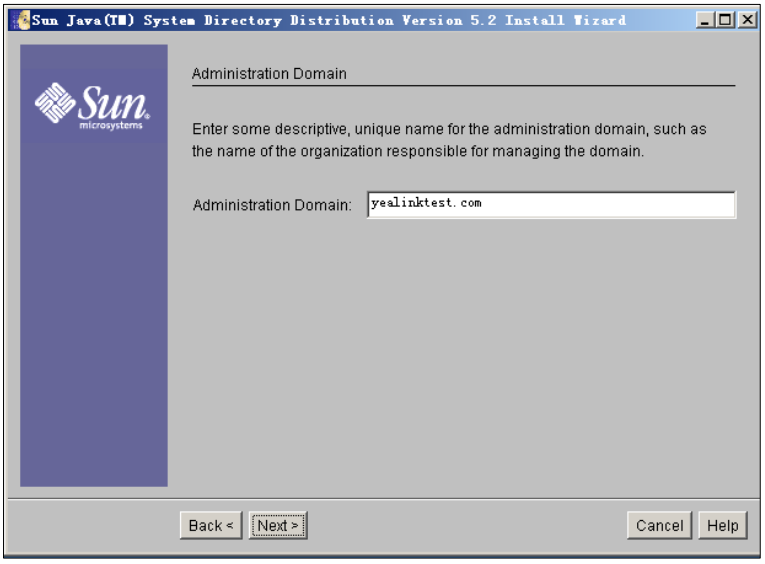
12. Enter the value "ldapsun" in the **Server Identifier** field and keep the default values in the other two fields. And then click **Next**.



13. Configure the password for the Directory Server Administrator and click **Next**.

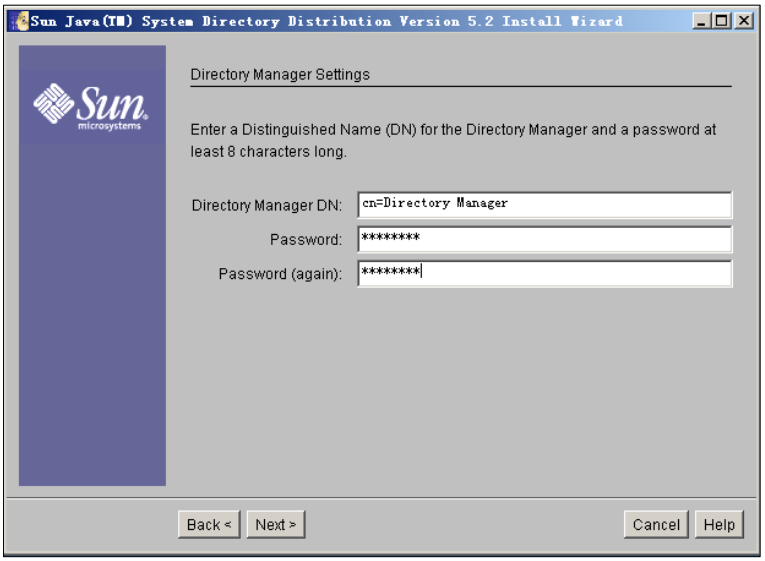


14. Follow the default setting and click **Next.**

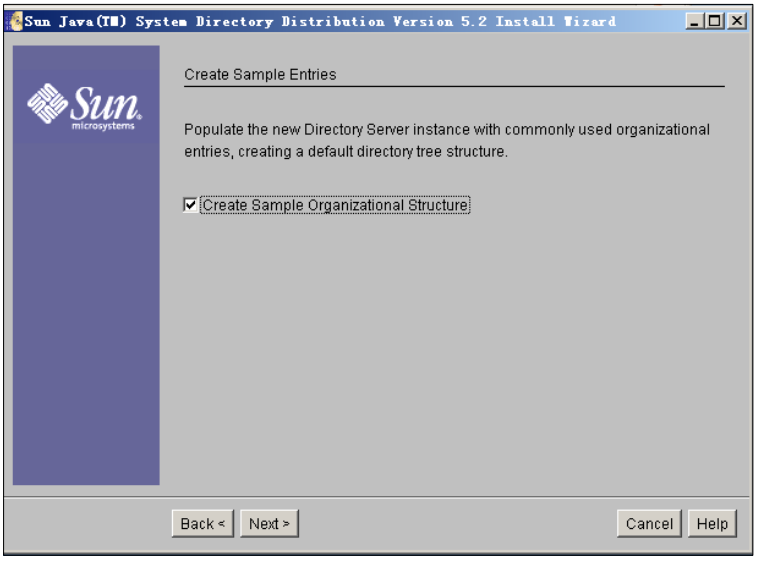


15. Configure the password for the Directory Manager and click **Next**.

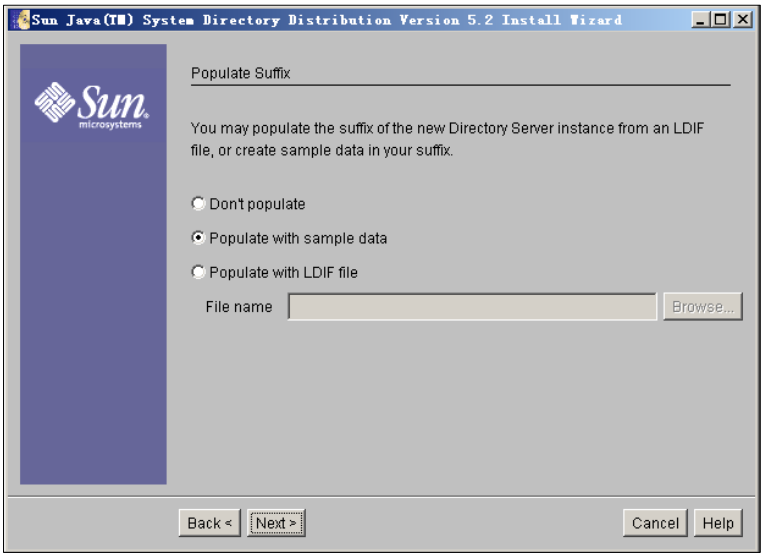
The password must be at least 8 characters long.



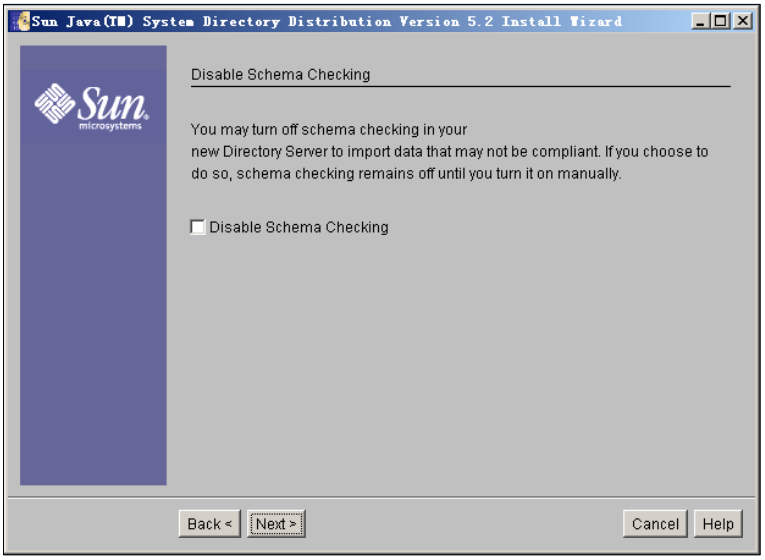
16. Check the **Create Sample Organizational Structure** check box and click **Next**.

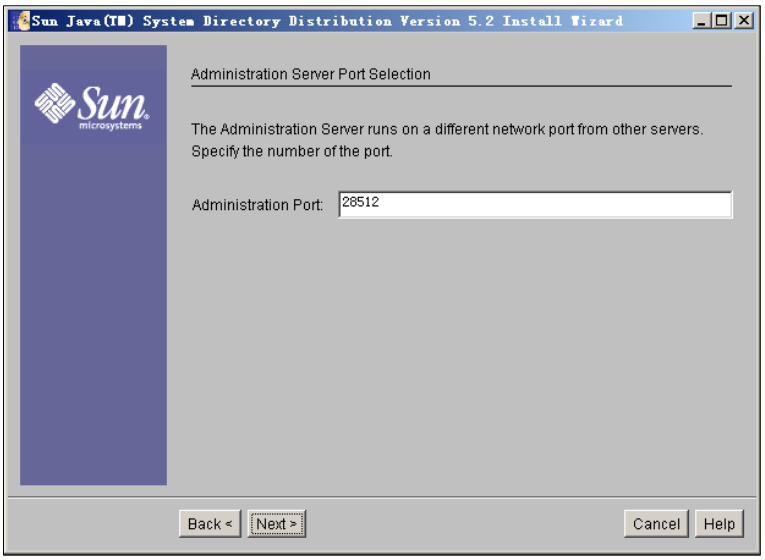


17. Mark the **Populate with sample date** radio box and click **Next**.

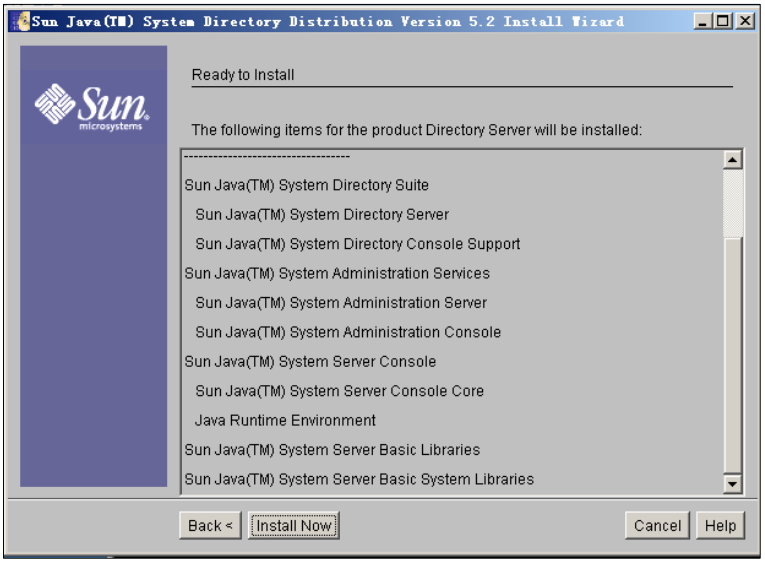


18. Follow the default settings and click **Next** for the following two steps.

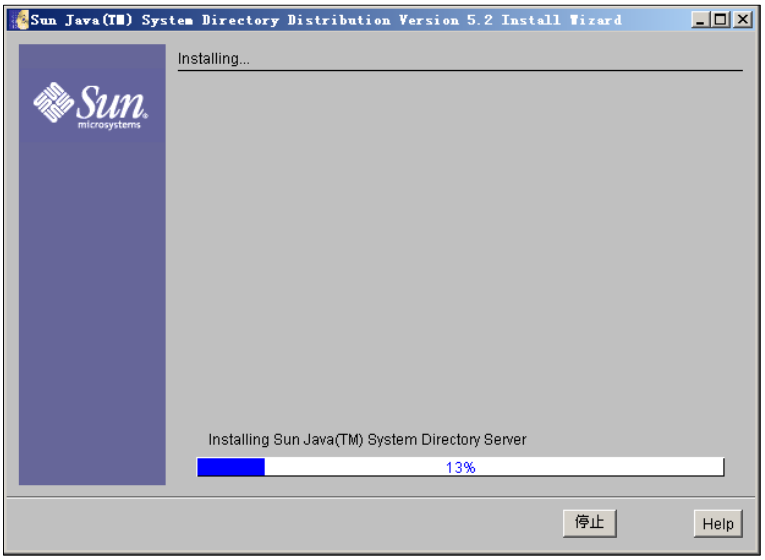




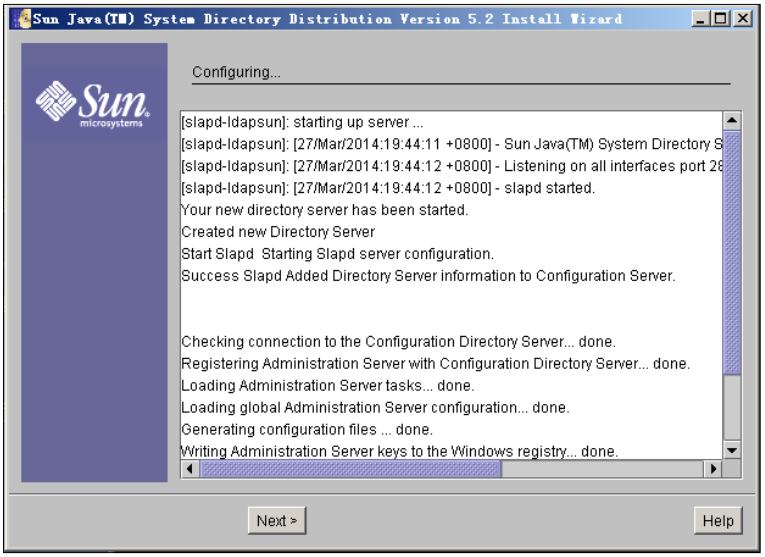
19. View the items to be installed and click **Install Now**.



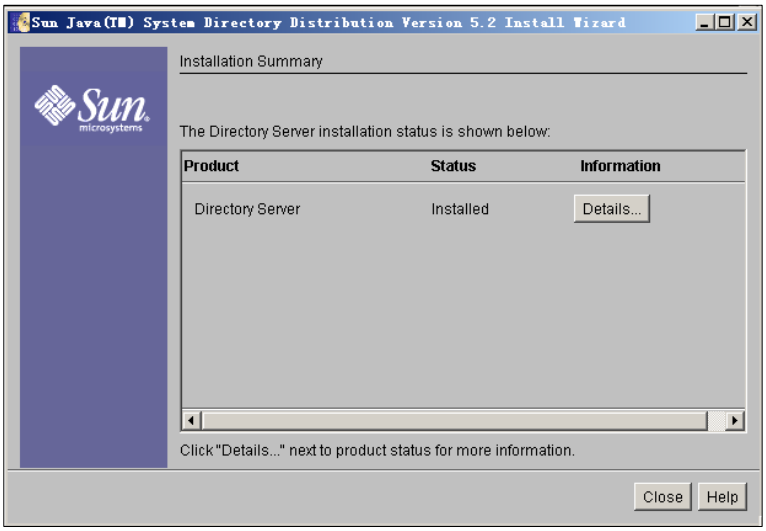
The installing progress is shown as below:



After the installation, it will enter the configuring screen.



20. After the configuration, click **Next** to enter the installation summary screen. You can view the directory server installation status and click **Details** for more information. You can also click **Close** to close the Sun Java(TM) System Directory Distribution Version 5.2 Install Wizard.



Configuring the Sun Java(TM) System Server Console

Adding an Entry to the Directory Server

You can add entries to the Directory Server one by one in this way.

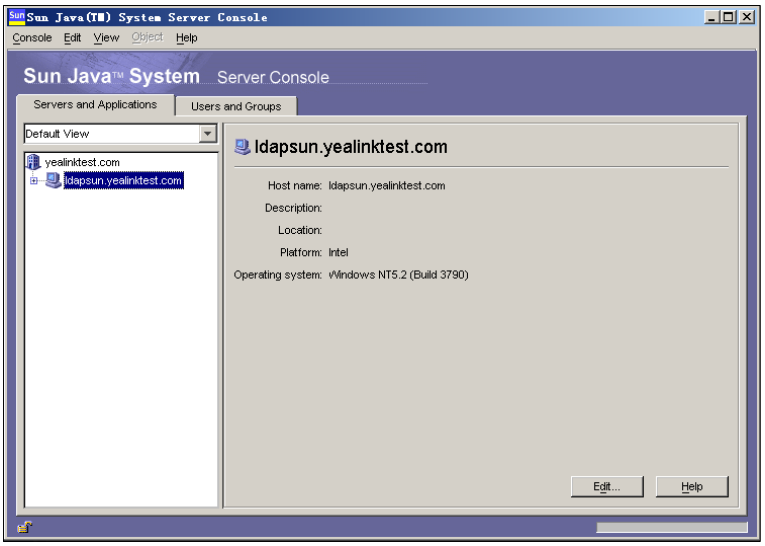
To add an entry to the Directory Server:

1. Click **Start**->**Program**->**Sun Java(TM) System Server Products**->**Sun Java(TM) System Server Console 5.2**.

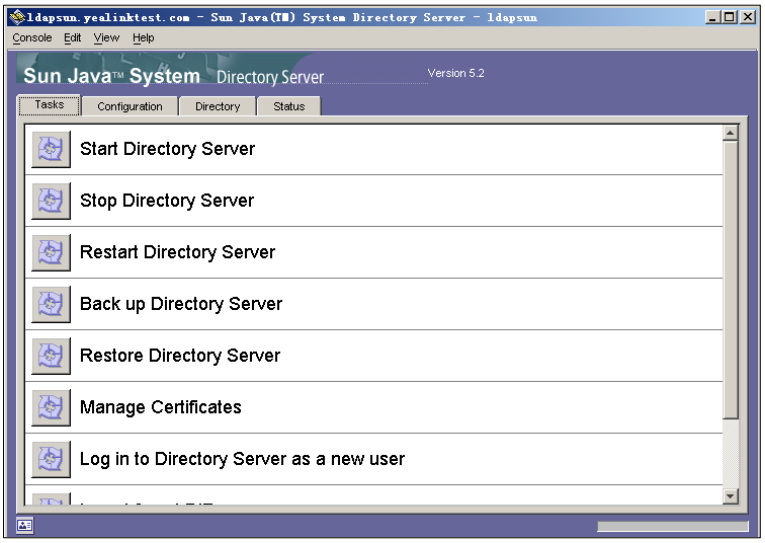
It will enter the login screen. You should enter the administrator user name and its password in the **User ID** field and **Password** field respectively.

The system default administrator is cn=Directory Manager and its password which must be at least 8 characters long has already been set during the installation process.

Then click **OK** to enter the home page.

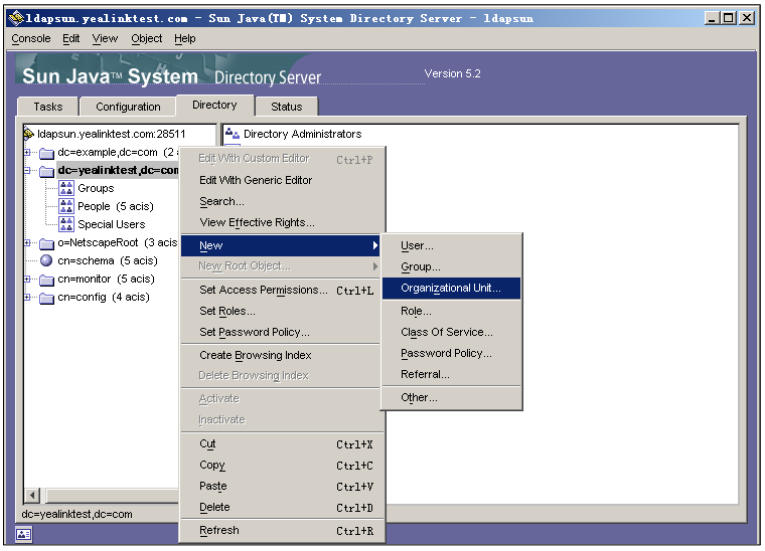


2. Double click **ldapsun.yealinktest.com**->**Server Group**->**Directory Server(ldapsun).** It will enter the Directory Tasks interface.

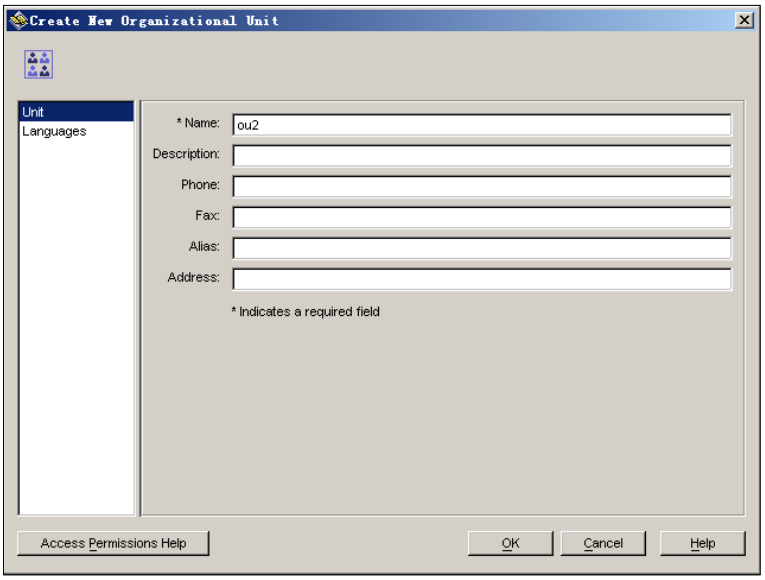


3. Click the **Directory** tab**.**

4. Select and right-click the **dc=yealinktest,dc=com (6 acis)**, and then select **New**->**Organizational Unit**.

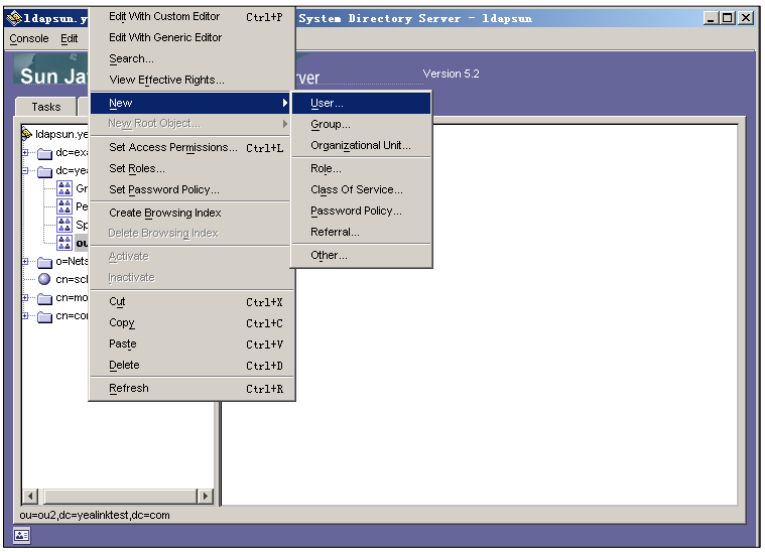


5. Enter the desired name of the organizational unit.

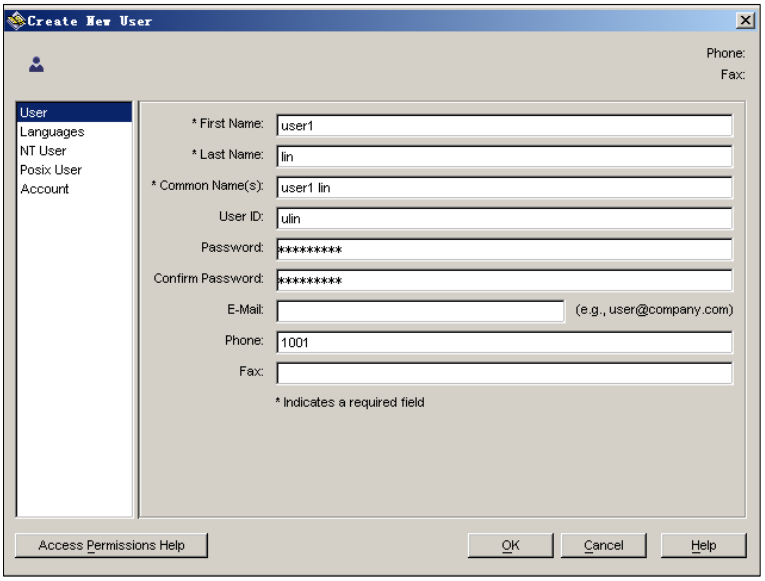


6. Click **OK** to accept the change.

7. Select and right-click the organizational unit created above, and then select **New**->**User**.

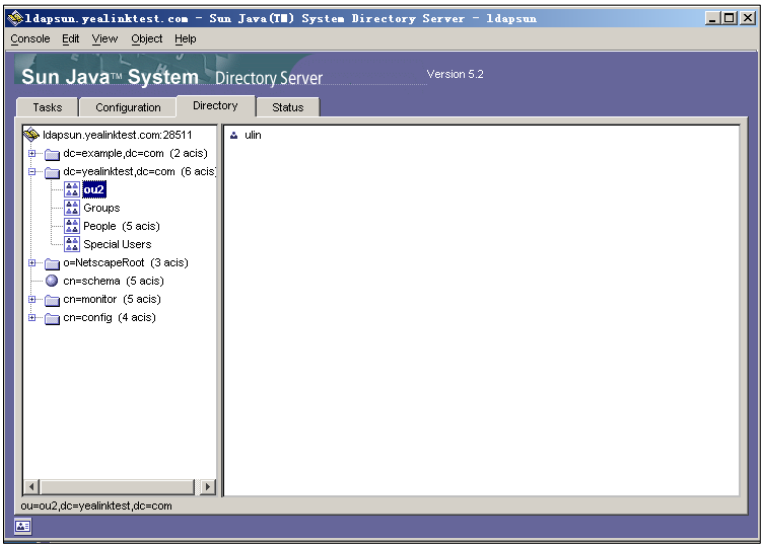


8. Enter the desired values in the corresponding fields.



9. Click **OK** to accept the change.

You can view the user (User ID is ulin) created above under the organizational unit named ou2.



Adding Entries to the Directory Server Using the ldifde Tool

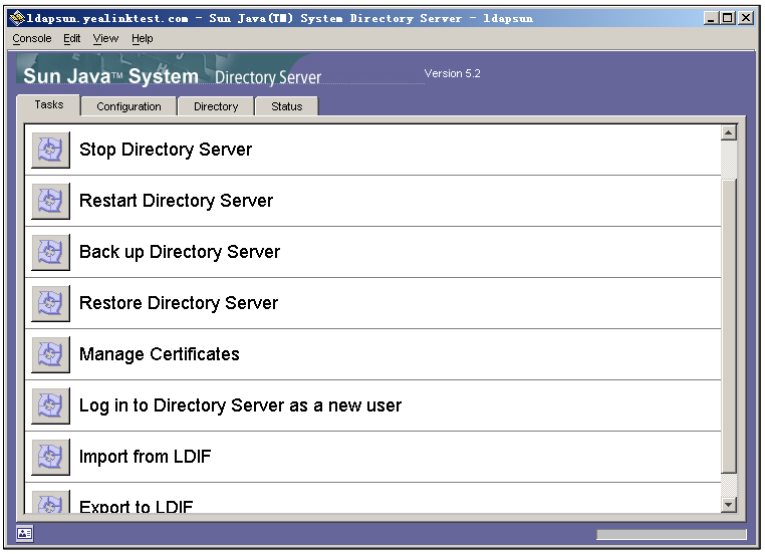
You can use an LDIF file to perform a batch import of all entries to the Directory Server. For more information, refer to create the LDIF file. The following shows an example of the content of the LDIF file for the Directory Server:

```
##Create a new organizational unit##
dn: ou=ou3,dc=yealinktest,dc=com
ou: ou3
objectClass: top
objectClass: organizationalunit
creatorsname: cn=directory manager
modifiersname: cn=directory manager
parentid: 1
entryid: 15
entrydn: ou=ou3,dc=yealinktest,dc=com

##create a new user##
dn: uid=utest,ou=ou3,dc=yealinktest,dc=com
uid: utest
facsimileTelephoneNumber: 11002
givenName: user4
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetorgperson
sn: test
cn: user4 test
```

To import the test.ldif file:

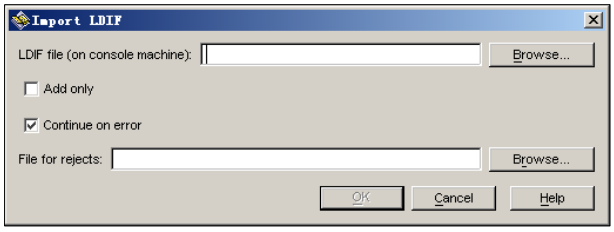
1. On the home page of Sun Java(TM) System Server Console, double click **ldapsun.yealinktest.com->Server Group->Directory Server(ldapsun).**

   It will enter the Directory Tasks interface.

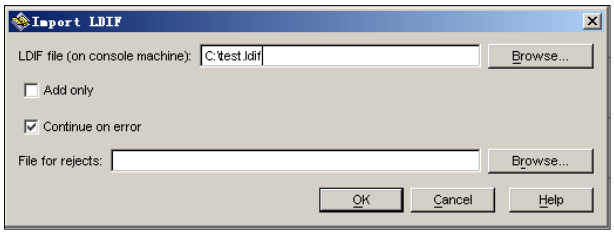


2. Click **Import from LDIF**.

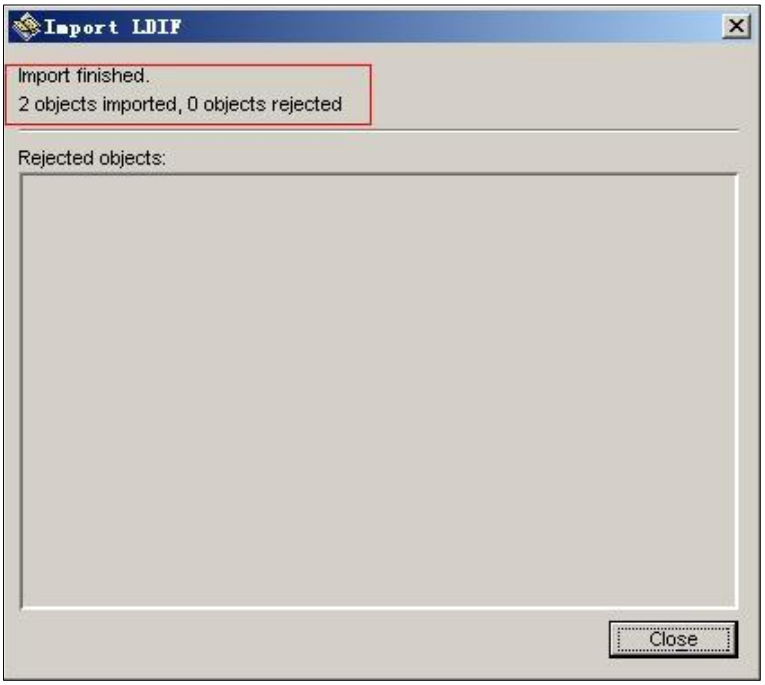
   It prompts the following dialog box.



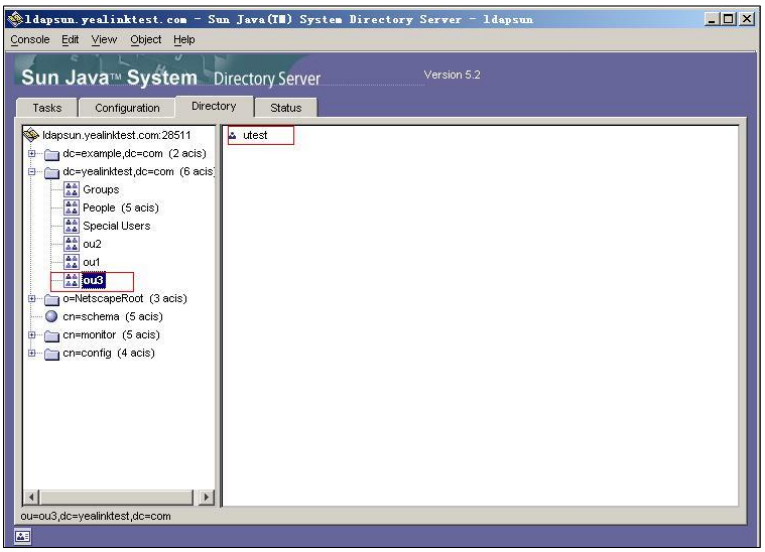
3. Click **Browse** to locate the test.ldif file from your local system, and then click **OK**.



After importing the test.ldif file, it will show the status of importing. If the entries are added successfully, you can view the information "n objects imported, 0 objects rejected". You can click **Close** to close it.



You can view the imported the organizational unit (e.g., ou3) and user (e.g., uid=utest) under the path: **Directory**-> **dc=yealinktest,dc=com (6 acis).**



Configuring Yealink IP Phones

LDAP is disabled on IP phones by default. You can configure LDAP via the web user interface or using configuration files.

LDAP Attributes on the Phone

Enable LDAP	
Parameter	ldap.enable
Description	This parameter enables or disables the LDAP feature on the IP phone. **0**-Disabled (Default) **1**-Enabled
LDAP Search	
Parameter	ldap.search_type
Description	This parameter configures the search type for the LDAP contact lookup. **0**-Prefix matching **1**-Approximate string matching If it is set to 0 (Perfect matching), the IP phone will search the LDAP contacts that the phone number or name starts with the entered character(s). If it is set to 1 (Approximate string matching), the IP phone will search the LDAP contacts that the phone number or name contains the entered character(s).
LDAP Name Filter	
Parameter	ldap.name_filter
Description	This parameter specifies the search criteria for names lookup. The format of the search criteria is compliant to the standard string representations of LDAP search filters (RFC 2254). The "*" symbol in the filter stands for any character. The "%" symbol in the filter stands for the name entered by the user.
Example	• (|(cn=%)(sn=%)(telephoneNumber=%)) When the cn or sn or telephoneNumber of the LDAP contact matches the entered name, the record will be displayed on the phone LCD screen. • (&(cn=*)(sn=%)) When the cn of the LDAP contact is set and the sn of the LDAP contact matches the entered name, the records will be displayed on

	the phone LCD screen. ● (!(cn=%)) When the cn of the LDAP contact does not match the entered name, the records will be displayed on the phone LCD screen.
LDAP Number Filter	
Parameter	ldap.number_filter
Description	This parameter specifies the search criteria for numbers lookup. The format of the search criteria is compliant to the standard string representations of LDAP search filters (RFC 2254). The "*" symbol in the filter stands for any number. The "%" symbol in the filter stands for the number entered by the user.
Examples	● (|(telephoneNumber=%)(mobile=%)(ipPhone=%)) When the telephoneNumber or mobile or ipPhone of the LDAP contact matches the search criteria, the record will be displayed on the phone LCD screen. ● (&(telephoneNumber=*)(mobile=%)) When the telephoneNumber of the LDAP contact is set and the mobile of the LDAP contact matches the entered number, the record will be displayed on the phone LCD screen.
LDAP TLS Mode	
Parameter	ldap.tls_mode
Description	This parameter specifies the connection mode between the LDAP server and the IP phone. **0**-LDAP (Default)−Unencrypted connection between the LDAP server and the IP phone. (port 389 is used by default). **1**-LDAP TLS Start−TLS/SSL connection between the LDAP server and the IP phone (port 389 is used by default). **2**-LDAPs−TLS/SSL connection between the LDAP server and the IP phone (port 636 is used by default). **Note:** It is only applicable to IP phones running firmware version 73 or later.
Server Address	
Parameter	ldap.host
Description	This parameter specifies the domain name or IP address of the LDAP server.
Default Value	Blank
Example	● 10.3.6.128

	• ldap.company.com
Port	
Parameter	ldap.port
Description	This parameter specifies the LDAP server port.
Default Value	389
Base	
Parameter	ldap.base
Description	This parameter specifies the LDAP search base which corresponds to the location in the LDAP directory. The search base narrows the search scope and decreases directory search time.
Example	• dc=yealink,dc=com
Username	
Parameter	ldap.user
Description	This parameter specifies the user name to login to the LDAP server. If the LDAP server allows anonymous to log in, this parameter can be left blank. Otherwise, you need to provide the user name to access the LDAP server. **Note:** If you use Microsoft Active Directory Application Mode (ADAM) as the LDAP server, the user to log in the LDAP server must be added to the administrator group in advance.
Password	
Parameter	ldap.password
Description	This parameter specifies the password to login to the LDAP server. If the LDAP server allows anonymous to log in, this parameter can be left blank. Otherwise, you need to provide the password to access the LDAP server.
Max Hits (1~32000) **For T48U/T48S/T46U/T46S/T43U/T42S/T41S/T40P/T40G/T27G/T23P/T23G/T21(P) E2/T19(P) E2/CP920:** **Max Hits (1~1000)**	
Parameter	ldap.max_hits
Description	This parameter specifies the maximum number of the search results to be returned by the LDAP server. If the value of the “Max.Hits” is blank, the LDAP server will return all searched results. Please note that a very large value of the “Max. Hits” will slow down the LDAP search speed, therefore the parameter should be configured according to the available bandwidth.
Default Value	50

LDAP Name Attributes	
Parameter	ldap.name_attr
Description	This parameter specifies the name attributes of each record to be returned by the LDAP server. This parameter compresses the search results. The user can configure multiple name attributes separated by space.
Example	● cn sn displayName This requires the "cn", "sn" and "displayName" attributes set for each contact record on the LDAP server. ● givenName This requires the "givenName" attribute set for each contact record on the LDAP server.
LDAP Number Attributes	
Parameter	ldap.numb_attr
Description	This parameter specifies the number attributes of each record to be returned by the LDAP server. This parameter compresses the search results. The user can configure multiple number attributes separated by space.
Example	● mobile telephoneNumber ipPhone This requires the "mobile", "telephoneNumber" and "ipPhone" attributes set for each contact record on the LDAP server.
LDAP Display Name	
Parameter	ldap.display_name
Description	This parameter specifies the display name of the contact record displayed on the LCD screen. This parameter value must start with a "%" symbol.
Example	● %cn The desired display name of the contact record is the cn attribute.
Protocol	
Parameter	ldap.version
Description	This parameter specifies the LDAP protocol version supported on the phone. Make sure the protocol value corresponds with the version assigned on the LDAP server. **2**-Version 2 **3**-Version 3 (Default)
LDAP Lookup For Incoming Call	
Parameter	ldap.call_in_lookup

Description	This parameter enables or disables the phone to perform an LDAP search when receiving an incoming call. **0**-Disabled (Default) **1**-Enabled **Note**: If the caller number contains the special characters (e.g., "+", "." or space), the phone will match the search criteria in the parameter "LDAP Name Filter (ldap.name_filter)". If not, the phone will match the search criteria in the parameter "LDAP Number Filter (ldap.number_filter)".
LDAP Lookup For Callout	
Parameter	ldap.call_out_lookup
Description	This parameter enables or disables the phone to perform an LDAP search when placing a call. **0**-Disabled (Default) **1**-Enabled **Note**: If the called number contains the special characters (e.g., "+", "." or space), the phone will match the search criteria in the parameter "LDAP Name Filter (ldap.name_filter)". If not, the phone will match the search criteria in the parameter "LDAP Number Filter (ldap.number_filter)".
LDAP Sorting Results	
Parameter	ldap.ldap_sort
Description	This parameter enables or disables the phone to sort the search results in alphabetical order or numerical order. **0**-Disabled (Default) **1**-Enabled
LDAP Special Search	
Parameter	ldap.incoming_call_special_search.enable
Description	This parameter enables or disables the phone to search the telephone numbers starting with "+" symbol and "00" from the LDAP server if the incoming phone number starts with"+" or "00". When completing the LDAP search, all search results will be displayed on the LCD screen. **0**-Disabled (Default) **1**-Enabled For example, If the phone receives an incoming call from the phone number 0044123456789, it will search 0044123456789 from the LDAP server first, if no result found, it will search +44123456789 from the server again. The phone will display all the search results. **Note:** It works only if the value of the parameter "ldap.call_in_lookup" is

	set to 1 (Enabled). You may need to set the value of the parameter "ldap.name_filter" to be (|(cn=%)(sn=%)(telephoneNumber=%)(mobile=%)) for searching the telephone numbers starting with "+" symbol.
LDAP Label	
Parameter	ldap.customize_label
Description	It configures the display name of the LDAP phone book. **Example**: ldap.customize_label = Friends **Note:** It works only if "ldap.enable" is set to 1 (Enabled).

Configuring LDAP via Web User Interface

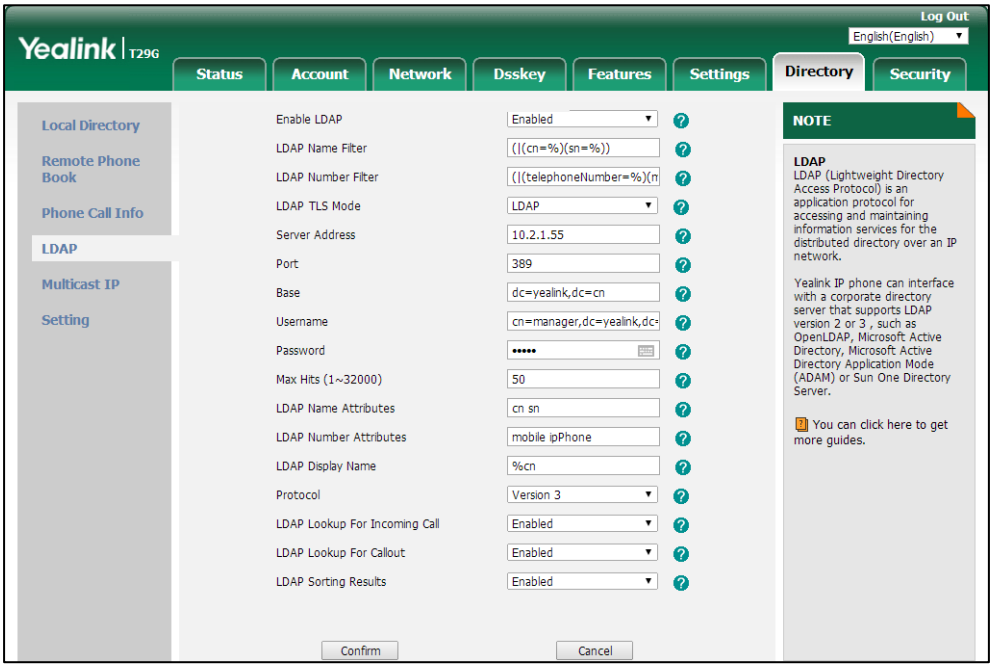
The following takes configurations of a SIP-T29G IP phone running firmware version 81 as examples.

To configure LDAP feature via web user interface:

1. Press the **OK** key on the phone when it is idle to obtain the IP address.
2. Enter the IP address (e.g., http://192.168.0.10 or 192.168.0.10) in the address bar of the web browser on your PC and then press **Enter**.
3. Enter the user name and password in the login page.

   The default login user name is admin (case-sensitive) and the password is admin (case-sensitive).
4. Click on **Directory**->**LDAP**.
5. Select **Enabled** from the **Enable LDAP** drop-down menu.

6. Enter the desired values in the corresponding fields.



7. Click **Confirm** to accept the change.

Example for Web User Interface Configuration

You can use the following settings as a starting point and adjust the filter and display attributes according to your requirements. The following shows an example of OpenLDAP phone configurations.

Enable LDAP: Enabled

LDAP Name Filter: (|(cn=%)(sn=%))

LDAP Number Filter: (|(telephoneNumber=%)(mobile=%)(ipPhone=%))

LDAP TLS Mode: LDAP

Server Address: 10.3.6.128

Port: 389

Base: dc=yealink,dc=com

Username: cn=Manager,dc=yealink,dc=com

Password: secret

Max Hits (1~32000): 50

LDAP Name Attributes: cn sn

LDAP Number Attributes: mobile telephoneNumber ipPhone

LDAP Display Name: %cn

Protocol: Version 3

LDAP Lookup For Incoming Call: Enabled

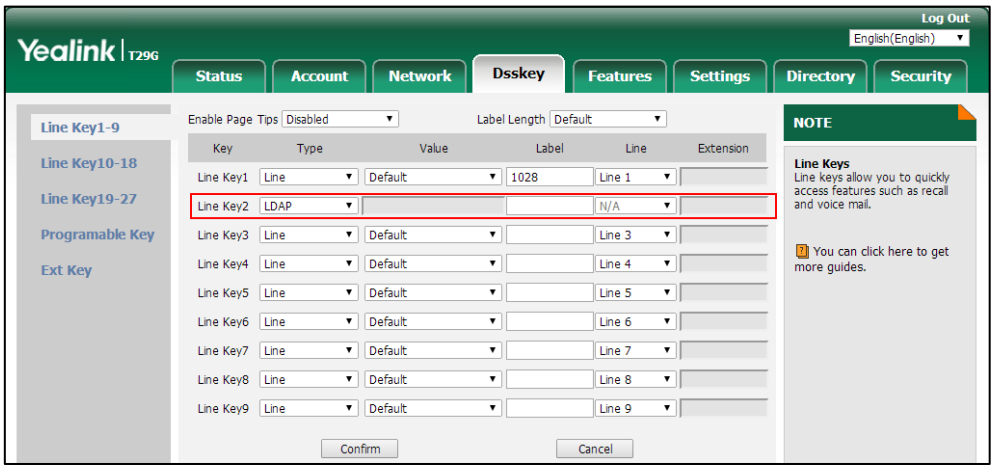
LDAP Lookup For Callout: Enabled

LDAP Sorting Results: Enabled

To use LDAP feature, you need to configure a DSS key as an LDAP key.

To configure an LDAP key via the web user interface (not applicable to W52P/W53P/W56P/W60P/CP930W-Base):

1. Log in to the web user interface of the phone.
2. Click on **Dsskey**->**Line Key** (or **Programmable Key**).
3. In the desired DSS key field, select **LDAP** from the **Type** drop-down menu.



4. Click **Confirm** to accept the change.

Configuring LDAP Using Configuration Files

To configure LDAP feature using configuration files:

1. Add/Edit LDAP parameters in the configuration file.

   The following table shows the information of parameters:

Parameter	Descriptions	Web Setting Path
ldap.enable	These parameters specify the LDAP attributes. Refer to the introduction above for more information.	Directory->LDAP->Enable LDAP
ldap.search_type (not applicable to CP860/CP920 IP phones)		/
ldap.customize_label		Directory->LDAP->LDAP Label
ldap.name_filter		Directory->LDAP->LDAP Name Filter
ldap.number_filter		Directory->LDAP->LDAP Number Filter
ldap.tls_mode		Directory->LDAP->LDAP TLS Mode

Parameter	Descriptions	Web Setting Path
ldap.host		Directory->LDAP->Server Address
ldap.port		Directory->LDAP->Port
ldap.base		Directory->LDAP->Base
ldap.user		Directory->LDAP->User Name
ldap.password		Directory->LDAP->Password
ldap.max_hits		Directory->LDAP->Max Hits
ldap.name_attr		Directory->LDAP->LDAP Name Attributes
ldap.numb_attr		Directory->LDAP->LDAP Number Attributes
ldap.display_name		Directory->LDAP->LDAP Display Name
ldap.version		Directory->LDAP->Protocol
ldap.call_in_lookup		Directory->LDAP->LDAP Lookup For Incoming Call
ldap.call_out_lookup		Directory->LDAP->LDAP Lookup For Callout
ldap.ldap_sort		Directory->LDAP->LDAP Sorting Results
ldap.incoming_call_special_search.enable		/

2. Upload configuration files to the root directory of the provisioning server and trigger IP phones to perform an auto provisioning for a configuration update.

For more information on auto provisioning, refer to the latest Auto Provisioning Guide on Yealink Technical Support.

Example for Configuration Parameters

You can use the following settings as a starting point and adjust the filter and display attributes according to your requirements. The following shows an example of OpenLDAP phone configurations.

```
ldap.enable=1
ldap.search_type = 1
ldap.name_filter= (|(cn=%)(sn=%))
ldap.number_filter= (|(telephoneNumber=%)(mobile=%)(ipPhone=%))
ldap.tls_mode=0
ldap.host= 10.3.6.128
ldap.port= 389
ldap.base= dc=yealink,dc=com
ldap.user= cn=Manager,dc=yealink,dc=com
ldap.password= secret
ldap.max_hits= 50
ldap.name_attr= cn sn
ldap.numb_attr= mobile telephoneNumber ipPhone
ldap.display_name= %cn
ldap.version= 3
ldap.call_in_lookup= 1
ldap.call_out_lookup= 1
ldap.ldap_sort= 1
```

To use LDAP feature, you need to configure a DSS key as an LDAP key.

To configure an LDAP key using configuration files:

1. Add/Edit the LDAP key parameters in the configuration file.

   You can configure a line key, a programmable key or an ext key as an LDAP key. The following table shows the information of parameters:

Parameter	Description	Value
linekey.X.type (not applicable to SIP-T19(P) E2/CP860/CP920/W52P/W53P/W56P/W60P/CP930W-Base IP phones) (CP960: X ranges from 1 to 30; SIP VP-T49G/SIP-T57W/T48U/T48G/T48S/T88V Pro/T88W(Pro)/T87W/T85W/T77U: X ranges from 1 to 29; VP59/SIP-T58A/T54W/T46U/T46G/T46S/T29G/T74W/	Configures a line key as an LDAP key on the IP phone.	38

Parameter	Description	Value
T74U/T73W: X ranges from 1 to 27; SIP-T42G/T42S/T41P/T41S: X ranges from 1 to 15; SIP-T53W/T53/T43U/T27G: X ranges from 1 to 21; SIP-T40P/T40G/ T23P/T23G: X ranges from 1 to 3; T21(P) E2: X ranges from 1 to 2)		
programablekey.X.type (not applicable to CP960/W52P/W53P/W56P/W60P/CP930W-Base IP phones) (VP59: X=1-4, 12-14, 17; SIP-T58A/T57W: X=1-4, 12-14, 17-18; SIP VP-T49G: X=1-4, 12-14; SIP-T54W/T48U/T48G/T48S/T46U/T46G/T46S/T88V Pro/T88W(Pro)/T87W/T85W/T77U: X=1-10, 12-14, 17-18; SIP-T53W/T53/T43U/T42G/T42S/T41P/T41S/T40P/T40G/T74W/T74U/T73W: X=1-10, 13, 17-18; SIP-T29G/T27G: X=1-14, 17-18; SIP-T23P/T23G/T21(P) E2: X=1-10, 14, 17-18; CP860/CP920: X=1-6, 9, 13)	Configures a programmable key as an LDAP key on the IP phone.	38
expansion_module.X.key.Y.type (only applicable to SIP-T58A/T57W/T54W/T53W/T48U/T48S/T48G/T46U/T46S/T46G/T43U/T29G/T27G/T88V Pro/T88W(Pro)/T87W/T85W/T77U/T74W/T74U/T73W IP phones) (SIP-T58A/T57W/T54W/T53W/T53/T48U/T46U/T43U/T88V Pro/T88W(Pro)/T87W/T85W/T77U/T74W/T74U/T73W, X=1-3, Y=1-60; SIP-T48S/T48G/T46S/T46G, X=1-6, Y=1-40; SIP-T29G/T27G, X=1-6, Y=1-20, 22-40)	Configures an ext key as an LDAP key on the IP phone.	38

2. Upload configuration files to the root directory of the provisioning server and trigger IP phones to perform an auto provisioning for a configuration update.

For more information on auto provisioning, refer to the latest Auto Provisioning Guide on Yealink Technical Support.

Using LDAP Directory on Yealink IP Phones

For SIP-T2 Series, T19(P) E2, T4 Series, T5 Series,T7 Series,T8 Series, and CP Series IP Phones

You can press the LDAP key to access the LDAP directory. Enter the desired numbers to match the search criteria for searching a contact from LDAP directory, add local contacts from LDAP directory, and dial a contact from LDAP directory. You can also enable the phone to perform an LDAP search when receiving an incoming call or dialing an outgoing call.

To search a contact from the LDAP directory:

1. Press the **LDAP** key to access the LDAP search screen.
   The LCD screen prompts "None".

2. Enter the search criteria.

   The contacts which match the search criteria will appear on the LCD screen.

3. Press ⌃ or ⌄ to select the desired contact.
4. Do one of the following:
   - Press the **Option** soft key and then select **Detail** to view the detail information of the contact.

- Press the **Option** soft key and then select **Add to Contact** to add the contact to local.
- Press the **Send** soft key to dial out.

If the **LDAP Lookup For Incoming Call** parameter is enabled on the phone, the phone will perform an LDAP search when receiving an incoming call. If there is a contact record that matches the caller ID, the contact name will be displayed on the phone LCD screen as the calling line identification.

The screenshot of the LCD screen for reference is shown as below:

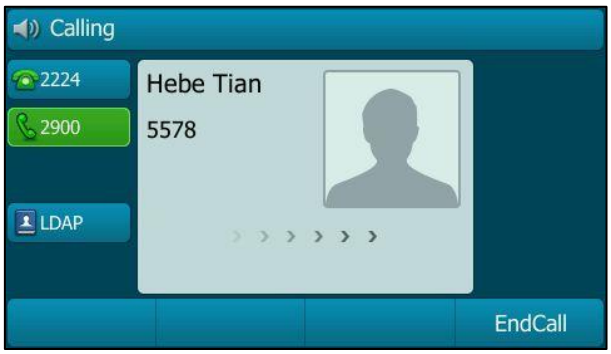
The **Search Source List In Dialing** feature enables the phone to perform an LDAP search when you enter the digits using the keypad in the dialing interface. For more information on the configuration of the Search Source List In Dialing feature, refer to *Yealink phone-specific user guide*.

If contact records are matching the search criteria, the contact records will be listed on the phone LCD screen. You can select the desired contact record to dial out. The contact name will be displayed on the phone LCD screen during the call.

The screenshot of the LCD screen for reference is shown as below:

If the **LDAP Lookup For Callout** parameter is enabled on the phone, the phone will perform an LDAP search when dialing an outgoing call. If there is a contact record that matches the called ID, the contact name will be displayed on the phone LCD screen as the called line identification.

The screenshot of the LCD screen for reference is shown as below:



For DECT IP Phones

You can access to the LDAP directory and enter the desired numbers to match the search criteria for searching a contact, add local contacts from LDAP directory, and dial a contact from LDAP directory. You can also enable the DECT phone to perform an LDAP search when receiving an incoming call or dialing an outgoing call.

The following takes the W53P running firmware version 83 as an example.

To search a contact from the LDAP directory:

1. Press **OK**->**Directory**->**LDAP**.

   The LCD screen of the handset displays the contact list.

2. Enter a few continuous characters of the contact name or continuous digits of the contact phone number using the keypad.

   The contacts which match the search criteria will display on the LCD screen.

3. Press ▲ or ▼ to select the desired contact.

4. Do one of the following:

   - Press the **Options** soft key and then select **Detail** to view the detail information of the contact.
   - Press the **Options** soft key and then select **Add to Local** to add the contact to local.
   - Press or to dial out.

If the **LDAP Lookup For Incoming Call** parameter is enabled on the DECT phone, the DECT phone will perform an LDAP search when receiving an incoming call. If there is a contact record that matches the caller ID, the contact name will be displayed on the handset LCD screen as the calling line identification.

The **Search Source List In Dialing** feature enables the phone to perform an LDAP search when you enter the digits using the keypad in the dialing interface. For more information on the

configuration of the Search Source List In Dialing feature, refer to Yealink phone-specific user guide.

If contact records are matching the search criteria, the contact records will be listed on the handset LCD screen. You can select the desired contact record to dial out. The contact name will be displayed on the handset LCD screen during the call.

If the **LDAP Lookup For Callout** parameter is enabled on the DECT phone, the DECT phone will perform an LDAP search when dialing an outgoing call. If there is a contact record that matches the called ID, the contact name will be displayed on the handset LCD screen as the called line identification.

Customer Feedback

We are striving to improve our documentation quality and we appreciate your feedback. Email your opinions and comments to DocsFeedback@yealink.com.