Using LDAP Phonebook on SIP-T46G IP Phones

Table of Contents

Introduction	1
Installing and Configuring the LDAP Server	3
OpenLDAP	3
Installing the OpenLDAP Server	3
Configuring the OpenLDAP Server	4
Configuring the LDAPExploreTool2	8
Microsoft Active Directory	
Installing the Microsoft Active Directory Server	
Installing Active Directory Lightweight Directory Services Role	
Configuring the Microsoft Active Directory Server	21
Configuring Yealink IP Phones	30
Using LDAP Phonebook	37

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 common name, or "mail" for 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 LDAP directory tree using traditional naming.



LDAP lets you "locate organizations, individuals, and other resources such as files and devices in a network, whether on the Internet or on a corporate intranet," and whether

1

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.

Yealink IP phones with the firmware version 61 or higher support the LDAP feature. This guide provides the configurations on the LDAP server and the SIP-T46G IP phones running the firmware version 71.

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 or Microsoft Active Directory in windows system.

OpenLDAP

Installing the OpenLDAP Server

This section shows you how to install an OpenLDAP server. The OpenLDAP server software is available for free. You can download it from http://www.openldap.org/software/download/.

To install the OpenLDAP server:

- 1. Double click the OpenLDAP application to start the installation. Follow the default settings and click **Next**.
- 2. Click **Browse** to locate the installation path from local computer system and then click **Next**.

You need to remember the installation path (e.g., C:\OpenLDAP) located here. The screenshot for reference is shown as below:



3. Select Full installation, the screenshot for reference is shown as below:

🚏 Setup - OpenLDAP	
Select Components Which components should be installed?	C.
Select the components you want to install; clear the component install. Click Next when you are ready to continue.	nts you do not want to
Full installation	_
 Install OpenLDAP openIdap-2.2.29 	10.7 MB 0.3 MB
Current selection requires at least 11.4 MB of disk space.	
< <u>B</u> ack	Next > Cancel

- 4. Follow the default settings and click Next.
- 5. Click Finish to finish the installation.

Configuring the OpenLDAP Server

Editing the slapd.conf File

Access the slapd.conf file at the OpenLDAP installation path. Open and edit the slapd.conf file using your favorite text editor.

1. Add the schema commands.

Find the command **include** ./schema/core.schema and add the following commands below it.

These two commands must be added:

include ./schema/cosine.schema

include ./schema/inetorgperson.schema

These commands can be added optionally:

./schema/corba.schema	
./schema/dyngroup.schema	
./schema/java.schema	
./schema/misc.schema	
./schema/nis.schema	
./schema/openIdap.schema	

2. Edit the manager information for LDAP phonebook.

Find the commands

Suffix "dc=my-domain, dc=com"

- Rootdn "cn=manager,dc=my-domain,dc=com"
- Rootpw secret

4

Suffix defines the components of the domain name.

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

Rootpw defines the user password of the management user.

For example:

Suffix "dc=yealink,dc=cn" Rootdn "cn=manager,dc=yealink,dc=cn" Rootpw secret

The suffix line means that the domain name of the LDAP phonebook is yealink.cn. The Rootdn line defines a management user named as manager. The Rootpw line defines the password "secret" for the management user.

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"

Rootpw secret

Starting the Slapd Server

To start the slapd server:

- 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 cd command to locate the server installation path. For example, execute cd c:\OpenLDAP to locate the server installation path at c:\OpenLDAP



4. Execute the command slapd -d 1 to start the slapd server.



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

The screenshot for reference is shown as below:



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

Adding the Initial Entry to the LDAP Directory

You can add the initial entry to the LDAP directory by 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=cn
objectclass: dcobject
objectclass: organization
o: xmyealink
dc: yealink
dn: cn=manager,dc=yealink,dc=cn
dc=yealink
objectclass: dcobject
objectclass: organization
cn=manager
sn: sumer

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.

- Execute the command cd c:\OpenLDAP to access the OpenLDAP installation path at c:\OpenLDAP.
- Execute the command Idapadd -x -D "cn=manager,dc=yealink,dc=cn" -w secret -f test.ldif to add the initial entry.

The screenshot for reference is shown as below:



Configuring the LDAPExploreTool2

The LDAPExploreTool2 application supports to run in windows system. The application in windows is a graphical LDAP tool that enables you to browse, modify and manage contact entry on 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 start the application.
- 2. Click File->Configurations.

LDAPEzplorerTool 2	
file Tools	- 21 - 12 - 14 - 14 - 14 - 14 - 14 - 14
Open last configuration	
Çonfigurations	
Quit 45	
	h

- 3. Click New to create a new configuration.
- 4. Enter a name in the **Configuration name** field under the **Configuration** tab.

Configuration		X
Configuration Server	Connection Option SSL/TLS	1
	ß	
Configuration name	LDAP	

5. Enter the domain name or IP address of the LDAP server in the Server name or IP field under the Server tab. Select to use the default port for the Server port and

8

		<i>k</i>
Server name or IP	10.2.11.162	μĘ
Server port	389	🔽 Use default port
Server SSL port	630	🔽 Use default port
Version	I → 3 ← 2	
	Test connection	1

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=cn"
```

Rootpw secret

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

User DN	cn-manager,dc-	🗖 Anonymous login
Password	*****	Store password
Use SSL port Use TLS	C Yes € No C Yes € No	(TLS is only used on non SSL ports)
Base DN	dc=yealink,dc=ci	Guess value

- 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

9. Click OK to accept the change.

Adding Entries

To add entries:

 Click File->Configurations, select the configuration created above, and then click Open.

The screenshot for reference is shown as below:

LDAPExplorerTool 2	
Root-dc=yealink, dc=cn	æ dc=yealink, dc=cn
	1.

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

LDAR	ExplorerTool 2		<
<u>F</u> ile <u>T</u> o	ools		
+ Root-	Entry	⊞- dc=yealink, dc=cn	
	Add		
	Copy to.hg		
	Rename		
	Delete		
	Search		
			/

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 own must attributes and may attributes. We select
Person from the pull-down list of Object class (from schema) for example.

4. Select the desired attributes for 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 is optional.

Attribute	Name	Description
cn	commonName	Full name of the entry.
gn	givenName	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.
0	organizationName	Organization name.
ου	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:

New entry creation			
Parent DN	dc=yealnk,dc=ci		
Entry RDN	cn=Hebe		
Object class (from schema)	person	•	
Object class (manual)		The value of cn her	o must ha tha
en			e most de the
🗉 cn-Hebe,dc-yealin	r a new value	same as the value	of cn configured
Tian cn Hel		in the Entry RDN fie	eld.
🖃 objectClass			
person E telephoneNumb		OK Cancel	
5570			
MUST attributes	MAY attr	ributes	
sn	userPass		
cn objectClass	telepho	neNumber	
bojeccento	descript	ion	
Attribute(when schema is unavailable)		Add	
is unavailable)			
	Save Can	rel	
		····	

- 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 catalogue.

Microsoft Active Directory

Installing the Microsoft Active Directory Server

This section shows you how to install an active directory on Microsoft windows server 2008 R2 Enterprise 64-bit.

To install the Microsoft active directory server:

- 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.

Active Directory Domain Services Installation Wizard	x
Choose a Deployment Configuration You can create a domain controller for an existing forest or for a new forest.	
C Existing forest	
old C Add a domain controller to an existing domain	
C Create a new domain in an existing forest This server will become the first domain controller in the new domain.	
Create a new domain in a new forest	
More about possible deployment configurations	
< Back Next >	Cancel

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

a Active Directory Domain Services Installation Wizard	×
Name the Forest Root Domain The first domain in the forest is the forest root domain. Its name is also the name of the forest.	
Type the fully qualified domain name (FQDN) of the new forest root domain.	
FQDN of the forest root domain:	
ldap.yealink.com	
Example: corp.contoso.com	
< Back Next > Ca	ancel

The wizard will check to see if the domain name is not already in use on the local network.

Active Directory	v Domain Services Installation Wizard	X
Name the Fores The first doma the forest.	t Root Domain in in the forest is the forest root domain. Its name is also the name of	
Type the fully	qualified domain name (FQDN) of the new forest root domain.	
FQDN of the f	orest root domain:	
Idap.yealink.c		_
Example: corp	Venfying NetBIOS name	
	< Back Next > Ca	ancel

7. Select the desired forest functional level from the pull-down list of Forest functional level, and click Next.

	ry Domain Services Installa nctional Level			
Select the fo	prest functional level.			
Forest functi	onal level:			
Windows S	erver 2003			•
Details:				
available in features: - Li ch - M by	vs Server 2003 forest functional Windows 2000 forest functional nked-value replication, which im nanges to group memberships. ore efficient generation of compl / the KCC. orest trust, which allows organiza	level, and the follo proves the replica ex replication top	owing additional ition of ologies	•
	You will be able to add only dom Windows Server 2003 or later to		t are running	
More about	domain and forest functional leve	<u>els</u>		
		< Back	Next >	Cancel

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

8. Select the desired domain functional level from the pull-down list of **Domain** functional level, and click **Next**.

For more information, click domain and forest functional levels.

Active Directory Domain Services Installation Wizard
Set Domain Functional Level Select the domain functional level.
Domain functional level:
Windows Server 2003
Details:
 The features available at the Windows Server 2003 domain functional level include ▲ all features available at the Windows Server 2000 domain functional level and the following additional features: Constrained delegation, which an application can use to take advantage of the secure delegation of user credentials by means of the Kerberos authentication protocol. lastLogonTimestamp updates: The lastLogonTimestamp attribute is updated with the last logon time of the user or computer, and it is
You will be able to add only domain controllers that are running Windows Server 2003 or later to this domain.
More about domain and forest functional levels
< Back Next > Cancel

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

ō Active Directory [Domain Services Installation Wizard	x
Set Domain Funct Select the doma	tional Level in functional level.	
Domain function	al level:	
Windows Serve	er 2003	▼
Details: The features i all features av following addi - Cor adv mea - last upo Yc More about <u>dom</u>	Examining DNS configuration	el include ▲ and the e is s ▼
	< Back	Next > Cancel

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

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

Active Directory	Domain Services Installation Wizard	×
Additional Domai	n Controller Options	
Select additiona	al options for this domain controller.	
DNS serve	ar -	
🔽 Global cat	alog	
🗖 Read-only	domain controller (RODC)	
Additional infor	mation:	
cannot be an We recommer controller.	RODC.	V
More about <u>ad</u>	lditional domain controller options < Back Next >	Cancel

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

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**.

Active	Directory Domain Services Installation Wizard	×
A	A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found or it does not run Windows DNS server. If you are integrating with an existing DNS infrastructure, you should manually create a delegation to this DNS server in the parent zone to ensure reliable name resolution from outside the domain petrilab.local. Otherwise, no action is required. Do you want to continue?	
	Yes No	

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.

Active Directory Domain Services Installation Wizard	×
Location for Database, Log Files, and SYSVOL. Specify the folders that will contain the Active Directory domain contro database, log files, and SYSVOL.	ller
For better performance and recoverability, store the database and log f volumes.	illes on separate
Database folder:	
C:\Windows\NTDS	Browse
Log files folder:	
C:\Windows\NTDS	Browse
SYSVOL folder:	
C:\Windows\SYSVOL	Browse
More about <u>placing Active Directory Domain Services files</u>	
< Back Next	> Cancel

12. Configure the password for the active directory recovery mode, click **Directory** Services Restore Mode password for more information and click Next.

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

a Active Directory Domain Services Inst	allation Wizard	×
Directory Services Restore Mode Adm	inistrator Password	
The Directory Services Restore Mode Ad Administrator account.	lministrator account is different from the	domain
Assign a password for the Administrator a controller is started in Directory Services choose a strong password.		
Password:	••••	
Confirm password:	••••	
More about Directory Services Restore N	lode password	
	< Back Next >	Cancel

13. Review your selection and click Next.

Active Directory Domain Services Installation Wizard	×
Summary	
Review your selections: Configure this server as the first Active Directory domain controller in a new forest. The new domain name is "Idap.yealink.com". This is also the name of the new forest. The NetBIOS name of the domain is "LDAP". Forest Functional Level: Windows Server 2003 Domain Functional Level: Windows Server 2003 Site: Default-First-Site-Name	▲
To change an option, click Back. To begin the operation, click Next. These settings can be exported to an answer file for use with other unattended operations. More about <u>using an answer file</u>	
< Back Next > C	ancel

The wizard will begin creating the Active Directory domain, and when finished, you will need to click **Finish** and reboot your computer.

Active Directory Domain Services Installation Wizard					
The wizard is configuring Active Directory Domain Services. This process can take from a few minutes to several hours, depending on your environment and the options that you selected.					
Securing Kerberos Policy					
Cancel					
Active Directory Demain Consider Testallation Witnesd					



Installing Active Directory Lightweight Directory Services Role

You should also install the Active Directory Lightweight Directory Services role on windows server 2008.

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 appear, click Next.

Add Roles Wizard		×
Before You Begin		
Before You Begin Server Roles Confirmation Progress Results	This wizard helps you install roles on this server. You determine which roles to install based on the tasks you want this server to perform, such as sharing documents or hosting a Web site. He doministrator account has a strong password He doministrator account has a strong password He tasks to count the as a trong password He tasks to count the state P addresses, are configured He tasks to count the state P addresses, are configured He tasks to count the state P addresses, are configured He tasks to count the proceeding steps, cancel the wizard, complete the steps, and then run the wizard again. To continue, dick Next.	
	< Previous Next > Install Cancel	

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

Select Server Roles Description Refore You Begin Select one or more roles to install on this server. Server Roles Role: Description: AD LDS Confirmation Active Directory Cetificate Services (Installed) Active Directory Cetificate Services (Installed) Progress Active Directory Lightweight Directory Services Active Directory Righte Management Services Active Directory Services Bold Server DHO' Server Progress Hyper-Y Active Orectory Forvices Application Services Hyper-Y Rework Deaktop Services Hyper-Y Network Policy and Access Services Hyper-Y Windows Deployment Services Windows Server Update Services Hyper-Y Hyper-Y Windows Server Update Services Windows Server Update Services Hyper-Y	Add Roles Wizard		×
Server Roles Description: AD LDS Active Directory Certificate Services Confirmation Progress Active Directory Certificate Services Choleston Frances Results Active Directory Uphweight Directory Services Active Directory Uphweight Directory Services Active Directory Roleston Services Active Directory Uphweight Directory Services Active Directory Uphweight Directory Services Progress Active Directory Uphweight Directory Services Active Directory Uphweight Directory Services DHOP Server DHOP Server DHOP Server File Services Prior and Document Services Prior and Document Services Prior Bestrop Services Remote Desktop Services Web Server (TIS) Web Service (TIS) Web Server (TIS) Web Services	Select Serv	ver Roles	
More about server roles <previous next=""> Instal Cancel </previous>	Server Roles AD LDS Confirmation Progress	Roles: Active Directory Certificate Services Active Directory Federation Services Active Directory Federation Services Active Directory Rights Management Services Application Server DKS Server File Services Print and Document Services Print and Document Services Web Server (IS) Windows Deployment Services Windows Deployment Services Windows Server Update Services Windows Server Idate Services	Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.

- 5. Follow the default settings and click Next.
- 6. When the installation ends, click Close.

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

E Server Manager		
File Action View Help		
⇐ 🔿 🖄 📷 🛛		
Server Manager (VL0215) Roles Active Directory Domain Services Features Peatures Configuration Storage	Roles Image: Wew the health of the roles installed or roles and features. Image: Roles Summary Image: Roles: 2 of 17 installed Image: Roles: 2 of 17 installed Image: Roles: 2 of 17 installed	on your server and add or remove Roles Summary Help Add Roles Remove Roles
	Active Directory Lightweight Directory Services Active Directory Domain Services	AD DS Help
	Stores directory data and manages communicat logon processes, authentication, and directory	tion between users and domains, includ
	Role Status	Go to Active Directory Dor Services
	Messages: 1 System Services: 9 Running, 1 Stopper	d v
	Last Refresh: Today at 13:00 Configure refre	sh

Configuring the Microsoft Active Directory Server

Adding a 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.
- Double click Roles->Active Directory Domain Services->Active Directory Users and Computers.
- Right click the domain name created above (e.g., Idap.yealink.com), and then select New->Organizational Unit.

Server Manager (YL0215)		Idap.yealink.com	6 objects [Filter /	Activated]	Actions	
Roles Active Directory I Active Directory I Active Directory I Active Directory Configuration Storage	Jomain Services ary Ukers and Computers [yl0215.ldap Delegate Control Find Change Domain Change Domain Controller Raise domain functional level Operations Masters	Name Builtin Computers Domain Cont ForeignSecur Managed Ser Users		Descriptio Default cc Default cc Default cc Default cc Default cc	Idap.yealink.com More Actions	
	New Al Tasks Al Tasks View Refresh Export List Properties Help	Computer Contact Group InetOrgPerson msImaging-PSPs MSMQ Queue Allas Organizational Unit Printer User Shared Folder				

4. Enter the desired name of the organizational unit.

New Object - Organizational Unit	×
Create in: Idap.yealink.com/	
Name:	
yealink	j
Protect container from accidental deletion	
OK Cancel	Help

- 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.

ew Object - Contact				
Create in:	ldap.yealink.com/Yealink			
First name:	san	Initials:	SZ	
Last name:	zhang			
Full name:	san sz. zhang			
Display name:				
		ОК		Cancel
		UK		Cancer

- 8. Click OK to accept the change.
- 9. Double click the contact created above.
- **10.** Configure more properties of the contact.

san sz. zhang Proper	ties	? ×
General Address T	elephones Organization Member Of	
san sz. z	hang	
First name:	san Initials: sz	
Last name:	zhang	
Display name:		
Description:		
Office:		
Telephone number: E-mail:	Other	
Web page:	Other	
	OK Cancel A	pply

11. Click OK to accept the change.

Adding Entries to the Active Directory Using the Idifde Tool

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

 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 the 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 content of the CSV file:

8	test. csv # X									
_	A	В	С	D	E	F	G	H	I	J
1	DN	objectClass	ou	name	cn	sn	givenName	initial s	ipPhone	mobile
2	OU=yealink,DC=ldap, DC=yealink,DC=com	organizationalUni t	yealink	yealink						
3	CN=san zhang, OU=yealink, DC =ldap, DC=yealink, DC =com	contact		san zhang	san zhang	san	zhang	sz	1111	123456789001
4	CN=si li,OU=yealink,DC=ld ap,DC=yealink,DC=co	contact		si li	si li	1i	si	sl	2222	123456789002
5	CN=wu wang,OU=yealink,DC= ldap,DC=yealink,DC= com	contact		wu wang	wu wang	wang	ΨU	₩₩	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 user.csv file. For example, execute **cd c:\Windows** to access the path of the user.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 idifde 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 or deny 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.
- Double click Server Manager->Roles->Active Directory Domain Services->Active Directory Users and Computers.
- **5.** 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.

ew Object - User	
Create in:	Idap.yealink.com/Users
First name:	san Initials: Sz
Last name:	zhang
Full name:	san sz. zhang
User logon name:	
Idapuser1	@ldap.yealink.com
User logon name (pre-	Windows 2000):
LDAP\	Idapuser1
	< Back Next > Cancel

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.

New Object - User	X
Create in: Idap.yealink.com/Users	
Password:	
Confirm password:	
☑ User must change password at next logon	
User cannot change password	
Password never expires	
Account is disabled	
< Back Next > Cancel	

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



Configuring Yealink IP Phones

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

To configure the 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 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 Contacts->LDAP.
- 5. Select Enabled from the pull-down list of Enable LDAP.
- 6. Enter the desired values in the corresponding fields.

The screenshot for reference is shown as below:

<i>l</i> ealink	Status	Account	Network	DSSKey	Features	Settings	Contacts	Security
		Enable LDAP		Enabled	•	1.0	NOTE	
Contacts		LDAP Name Filter		(((cn=%))(:	n=%))	0	Contacts LDAP	
Remote Phone Book		LDAP Number Filter		(I(telephor	eNumber=%)(M	0	Contacts LDAP	
Phone Call Info		Server Address		192.168.1.	30	0		
		Port		389		0		
LDAP		Base		dc=yealink,	dc=cn	0		
MulticastIP		Username		cn-manage	r,dc=yealink,dc+	0		
Setting		Password		•••••		0		
		Max. Hits (1~32000)	50		0		
		LDAP Name Attribut	tes	cn sn		0		
		LDAP Number Attrit	outes	Mobile teles	ohoneNumber ipf	0		
		LDAP Display Name		%cn		0		
		Protocol		Version3	•	0		
		LDAP Lookup For In	coming Call	Enabled	•	0		
		LDAP Sorting Result	s	Enabled	•	0		

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

LDAP Attributes on Web User Inter

Enable LDAP	
Description	This parameter enables the LDAP feature on the IP phone.
Valid Value	<enabled>, <disabled></disabled></enabled>
Default Value	Disabled
LDAP Name Filt	ter
Description	This parameter specifies the name attributes for LDAP searching. The format of the search filter 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 entering string used as the prefix of the filter condition.
Example	 ((cn=%)(sn=%)) When the name prefix of the cn or sn of the contact record matches the search criteria, the record will be displayed on the phone LCD screen. (&(cn=*)(sn=%)) When the name prefix of the sn of the contact record matches the search criteria, the record will be displayed on the phone LCD screen. (!(cn=%)) When the name prefix of the cn of the contact record does not match the search criteria, the record will be displayed on the phone LCD screen.
LDAP Number I	Filter
Description	This parameter specifies the number attributes for LDAP searching. The format of the search filter 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 entering string used as the prefix of the filter condition.
Examples	 ((telephoneNumber=%)(Mobile=%)(ipPhone=%)) When the number prefix of the telephoneNumber, Mobile or ipPhone of the contact record matches the search criteria, the record will be displayed on the phone LCD screen. (&(telephoneNumber=*)(Mobile=%)) When the number prefix of the Mobile of the contact record matches the search criteria, the record will be displayed on the phone LCD screen.

Server Address	
Description	This parameter specifies the domain name or IP address of the LDAP server.
Default Value	Blank
Example	• 192.168.1.100
	Idap.company.com
Port	
Description	This parameter specifies the LDAP server port.
Default Value	389
Base	
Description	This parameter specifies the LDAP search base which corresponds to the location in the LDAP phonebook. The search base narrows the search scope and decreases directory search time.
Example	• o=UNIVERSITY OF NEW ORLEANS,c=US
	• o=SFU,c=CA
	• dc=yealink,dc=cn
UserName	
Description	This parameter specifies the user name to login the LDAP server. If the LDAP server allows anonymous to login, this parameter can be
	left blank. Otherwise you need to provide the username to access the LDAP server.
Password	
Description	This parameter specifies the password to login the LDAP server. If the LDAP server allows anonymous to login, this parameter can be left blank. Otherwise you need to provide the password to access the LDAP server.
Max.Hits(1~32	000)
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 Att	ributes

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
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 N	lame
Description	This parameter specifies the display name of the contact record displayed on the LCD screen. This parameter value must start with "%" symbol.
Example	 %cn The desired display name of the contact record is the cn attribute.
Protocol	
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.
Valid Value	Version 2 or 3
Default Value	Version 3
LDAP Lookup F	or Incoming Call
Description	This parameter enables the phone to perform an LDAP search when receiving an incoming call.
Valid Value	<enabled>, <disabled></disabled></enabled>
Default Value	Disabled

LDAP Sorting Re	LDAP Sorting Results				
Description	This parameter enables the phone to sort the search results in alphabetical order or numerical order.				
Valid Value	<enabled>, <disabled></disabled></enabled>				
Default Value	Disabled				

Example for Configuration

You can use the following settings as a starting point and adjust the filter and display attributes according to your needs.

Enable LDAP: Enabled
LDAP Name Filter: ((cn=%)(sn=%))
LDAP Number Filter: ((telephoneNumber=%)(Mobile=%)(ipPhone=%))
Server Address: 192.168.1.30
Port: 389
Base: dc=yealink,dc=cn
UserName: cn=manager,dc=yealink,dc=cn
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 Sorting Results: Enabled

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

To configure an LDAP key via web user interface:

- 1. Log into the web user interface of the phone.
- 2. Click on DSSKey->Line Key.

3. In the desired DSS key field, select LDAP from the pull-down list of Type.

'ealink	Status		Account	Network	DS	SKey	Features	Settings	Contacts	Security
	Enable Page	Tips	Disabled	•					NOTE	
Line Key 1-9	Key		Туре	Value		Label	Line	Extension	DSSKEY Line	
Line Key 10-18	Line Key1	LDAP	•				N/A	-	DSSKEY LINE	ĸey
Line Key 19-27	Line Key2	Line	•	default	•		Line 2	•		
Programable Key	Line Key3	Line	•	default	•		Line 3	•		
· ·	Line Key4	Line	•	default	•		Line 4	•		
Ext Key	Line Key5	Line	•	default	¥		Line 5	•		
	Line Key6	Line	•	default	•		Line 6	•		
	Line Key7	N/A	•				N/A	-		
	Line Key8	N/A	•				N/A	-		
	Line Key9	N/A	•				N/A	-		

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

To configure the LDAP feature using the configuration file:

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

The following table shows the parameter information:

Parameter	Descriptions	Web Setting Path	
ldap.enable		Contacts->LDAP->Enable LDAP	
ldap.name_filter		Contacts->LDAP->LDAP Name Filter	
ldap.number_filter		Contacts->LDAP->LDAP Number Filter	
ldap.host	These parameters specify the LDAP	Contacts->LDAP->Server Address	
ldap.port	attributes. Refer to the	Contacts->LDAP->Port	
ldap.base	introduction above	Contacts->LDAP->Base	
ldap.user	for more information.	Contacts->LDAP->Username	
ldap.password		Contacts->LDAP->Password	
ldap.max_hits		Contacts->LDAP->Max. Hits (1~32000)	
ldap.name_attr		Contacts->LDAP->LDAP Name Attributes	
ldap.numb_attr		Contacts->LDAP->LDAP	

Parameter	Descriptions	Web Setting Path
		Number Attributes
ldap.display_name		Contacts->LDAP->LDAP Display Name
ldap.version		Contacts->LDAP->Protocol
ldap.call_in_lookup		Contacts->LDAP->LDAP Lookup For Incoming Call
ldap.ldap_sort		Contacts->LDAP->LDAP Sorting Results

2. Upload the configuration file to the root directory of the provisioning server and perform auto provisioning to configure the Yealink IP phones.

For more information on auto provisioning, refer to *Yealink SIP-T46G Auto Provisioning User Guide*.

To configure an LDAP key using the configuration file:

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

The following table shows the parameter information:

Parameter	Description	Value
linekey.x.type	Configures a line key to be LDAP key on the IP phone. X ranges from 1 to 27.	38

2. Upload the configuration file to the root directory of the provisioning server and perform auto provisioning to configure the Yealink IP phones.

For more information on auto provisioning, refer to *Yealink SIP-T46G Auto Provisioning User Guide*.

Using LDAP Phonebook

You can press the LDAP key to access the LDAP phonebook. Enter the search criteria to search a contact from LDAP phonebook, add local contacts from LDAP phonebook, and dial a contact from LDAP phonebook. You can also enable the phone to perform a LDAP search when dialing out or receiving an incoming call.

To search a contact form LDAP phonebook:

 Press the LDAP key to access the LDAP phonebook. The LCD screen prompts "None".



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

	L	DAP	0/1
h			
🔔 Hebe		1234	
Back	abc	Delete	

The contacts whose name or phone number matches the characters entered will appear on the LCD screen.

- 3. Press the navigation key to select the desired contact.
- 4. Do one of the following:
 - Press the **Option** soft key and then select to check the detail information of the contact.
 - Press the **Option** soft key and then select to add the contact to the local contact.

- Press the **dial** soft key to dial out.

If the LDAP Lookup For Incoming Call parameter is enabled for the phone:

The phone performs an LDAP search when receiving an incoming call. If there is a contact record which matches the caller ID, the contact name will be display 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 on the pre-dial interface. For more information on the configuration of the Search Source List In Dialing feature, refer to *Yealink SIP-T46G IP Phone User Guide*.

If there are contact records which match 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: