



keytalk

S/MIME LDAP

secure email address book

virtual appliance

admin setup manual

Company	KeyTalk IT Security
Author	MR van der Sman
Creation date	31 August 2018
Last updated	28 September 2020
Product	KeyTalk S/MIME LDAP secure e-mail address book
Data classification	Public
Software/firmware version	5.7.0
Manual version	5.7.0.3

Contents

1. KeyTalk's secure S/MIME email addressbook directory	3
2 Setup	4
2.1 Basic network configuration	4
2.2 KeyTalk LDAP management UI setup : activation and SSL	6
Step 1: Register your LDAP admin UI account	6
Step 2: Access the admin GUI.....	6
Step 3: Upload your valid KeyTalk license file to activate the LDAP functionality	6
Step 4: Change the LDAP HA sync password	7
Step 5: Change the LDAP admin password	7
Step 6: Set the ldap (node) FQDN hostname	9
Step 7: Install an SSL certificate	11
2.3 KeyTalk LDAP management UI: Network config.....	13
2.4 KeyTalk LDAP management UI: Admin strong authentication	14
2.5 KeyTalk LDAP management UI: High Availability	15
2.5.1 KeyTalk LDAP HA high over design.....	15
2.5.2 KeyTalk HA configuration.....	16
3 S/MIME LDAP secure email address book content	21
3.1 Directly accessing the LDAP for management	21
3.2 Writing KeyTalk managed certificates to the LDAP.....	21
3.3 Writing non-KeyTalk managed certificates to the LDAP	22
3.4 Restoring KeyTalk managed certificates to the LDAP	22
4 KeyTalk S/MIME LDAP as a web and mail client address book	23
4.1 Web based S/MIME email address book lookup	23
4.1 Webbased lookup basic look and feel change	23
4.2 Mail client based S/MIME email address book lookup.....	24
4.2.1 Automated mail client address book configuration.....	24
4.2.2 Manual mail client address book configuration	24
5 KeyTalk contact details and 3rd line support.....	25
 ANNEX A: Importing KeyTalk LDAP virtual appliance in AWS	26
ANNEX B: Importing KeyTalk LDAP virtual appliance in Azure	36

1. KeyTalk's secure S/MIME email address book directory

Many do not wish to fiddle with their own LDAP to make available their own secure public address book for S/MIME (encrypted email) detail lookup purposes for internal and external parties.

KeyTalk offers as part of its certificate and key management solution a hardened S/MIME LDAP public key server for the sole purpose of allowing people to lookup your enrolled S/MIME certificate details, and/or third party certificates you wish to securely send emails with, so these people can securely email those who are registered in the LDAP S/MIME address book.

This LDAP comes as a virtual appliance and allows for regular LDAP based address book lookups in commonly used email clients, but also includes a browser based lookup function based on Nginx.

As part of our security focus, this LDAP has been optimized to protect against harvest attacks by means of a return value of maximum 1, as a result this LDAP does NOT sync its entire contents to a requesting end-point.

Failed2ban (www.fail2ban.org) is incorporated and will block malicious IPs.

Advanced Network Intrusion Detection (<http://aide.sourceforge.net/>) is used to verify the integrity of files.

The specs:	Operating System:	CentOS 7.6.1810
	Kernel:	3.10.0-957.5.1.el7.x86_64
	OpenLDAP version:	slapd 2.4.44
	OpenSSL version:	1.0.2k-fips
	nGinx version:	1.12.2
	PHP version:	7.3.3
	Laravel version:	5.8.7
	Minimal memory requirement:	3 GB
	Preferred memory requirement:	8 GB
	Minimal CPU requirement:	2 cores, 4 threads
	Preferred CPU requirement:	4 cores, 8 threads
	Diskspace:	15 GB
	Lookups per second:	22.000 in optimal conditions
	Writes per second:	10.000 in optimal conditions
	Max S/MIME entries:	50.000.000
TCP in:	22	SSH by default not supported , only direct VM/Hypervisor CLI
	80	HTTP based certificate lookups
	389	LDAP only needed when non-secure lookups need to be supported
	443	HTTPS based email certificate lookup
	636	LDAPS needed for secure email certificate lookup
TCP out:	3000	Management UI access
	53	DNS
	80	KeyTalk virtual appliance
	123	NTP
	443	KeyTalk virtual appliance
	443	ldapupgrade.keytalk.com LDAP OS security update fetch
UDP out:	7999	stash.keytalk.com LDAP firmware updates (SSH protocol)
	514	Syslog/SIEM

2 Setup

2.1 Basic network configuration

DHCP is default used to assign networking.

To manually set your IP for the first time perform the following:

1) From your CLI login:

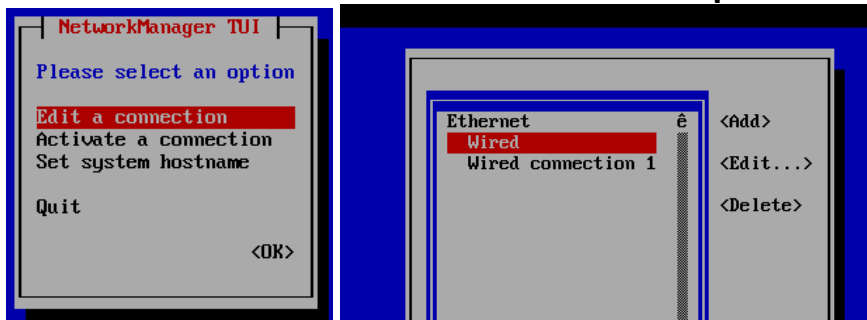
Username: keytalk

Password: Change!

2) After successful authentication the following options are provided:

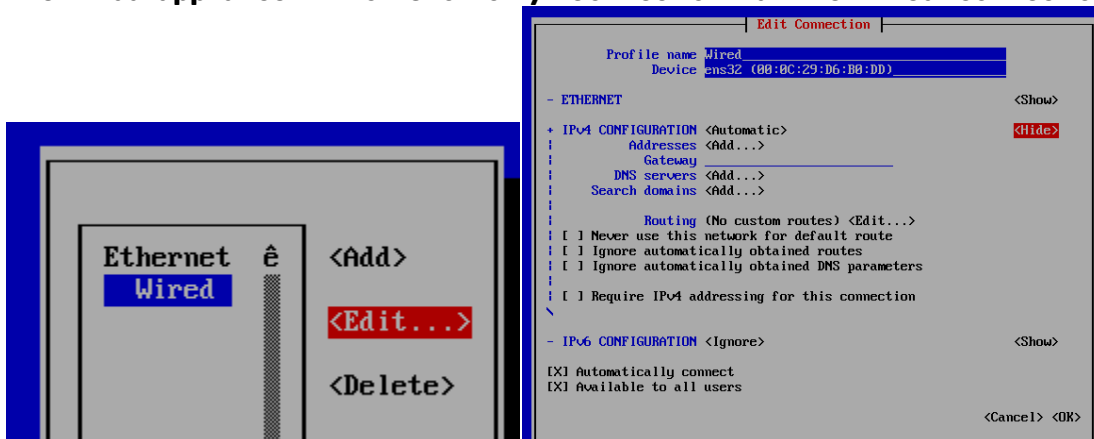
```
1) Show IP info
2) Setup network
3) Show running processes
4) Show blacklist
5) Reset to factory defaults
6) Set shell password
7) Reset Web-GUI password
8) Reset Firewall
9) Disable Firewall
10) Start Firewall
11) Disable client side SSL authentication
12) Refresh certificate
13) Show webserver log
14) Show system log
15) Configure syslog server
16) Update
17) Quit
Please enter your choice:
```

3) Select 2) to setup your network, and remove any shown connections, as Hypervisors tend to add unwanted additional connections on first time bootup.



Select OK, quit your virtual appliance, apply changes, login again, and setup network.

4) The virtual appliance will now show only 1 Connection. Edit the “Wired” connection:



Ensure you select: Manual and add the relevant networking

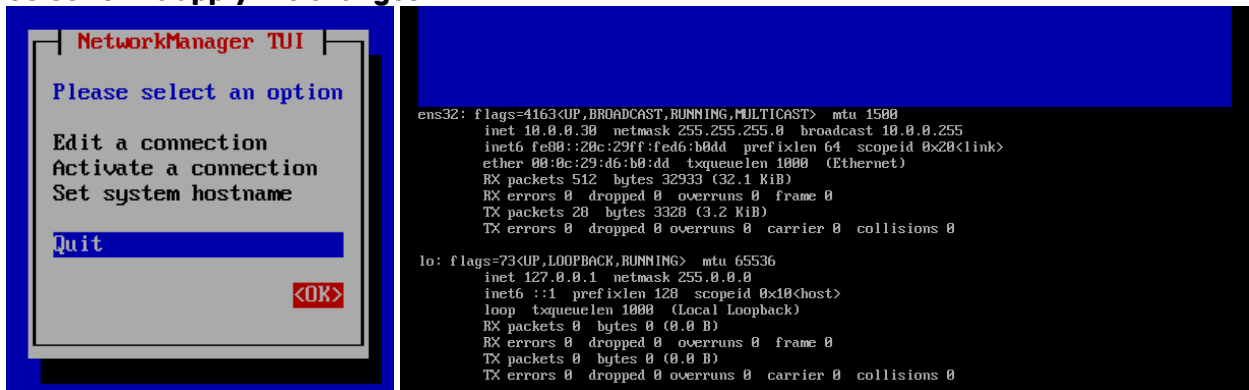
To set your subnetmask add the appropriate / (slash forward)to your IP, ref:

https://www.aelius.com/njh/subnet_sheet.html

NTP is fetched from the Hypervisor or from <https://time.is/UTC>

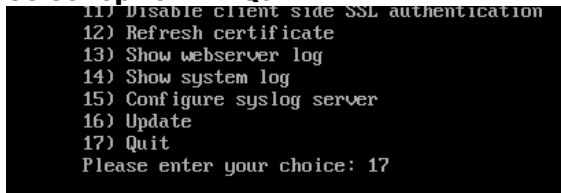
! DO NOT SET THE FQDN OR HOST NAME YET !

5) Select OK to apply the changes:

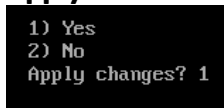


Press any key to return to the initial configuration menu

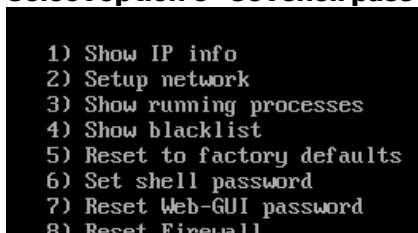
6) Select option 17 "Quit":



Apply the made changes:

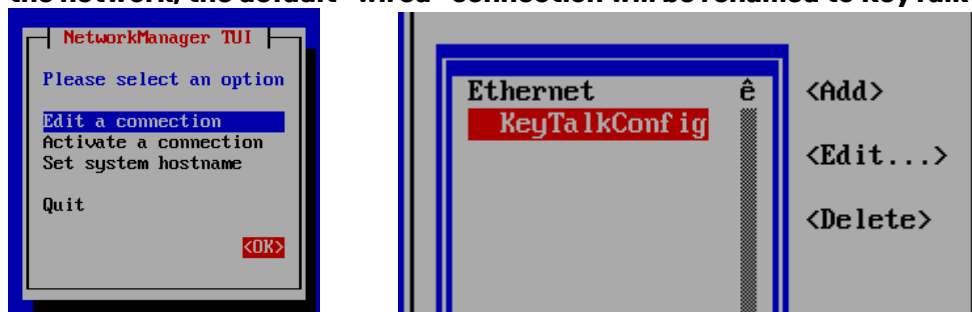


7) Select option 6 "Set shell password, to change your SSH password and remember it!"



NOTE:

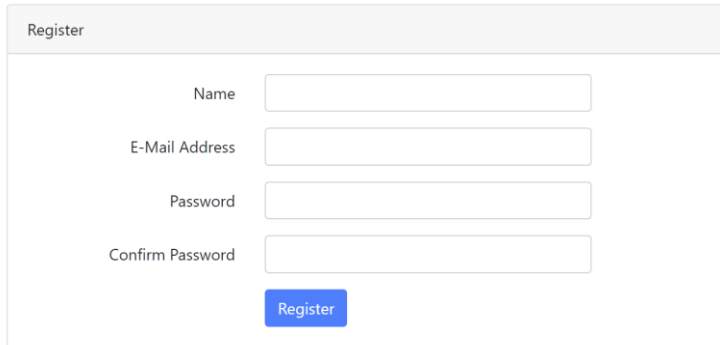
When the management web UI (port 3000/login) is used to at least once make changes to the network, the default "Wired" connection will be renamed to KeyTalkConfig



2.2 KeyTalk LDAP management UI setup : activation and SSL

In order to configure the actual LDAP functionality, perform the following steps:

Step 1: Register your LDAP admin UI account at: <https://<ip>:3000/register>

A registration form titled "Register" with a light gray header. It contains four input fields: "Name", "E-Mail Address", "Password", and "Confirm Password". Below the fields is a blue "Register" button.

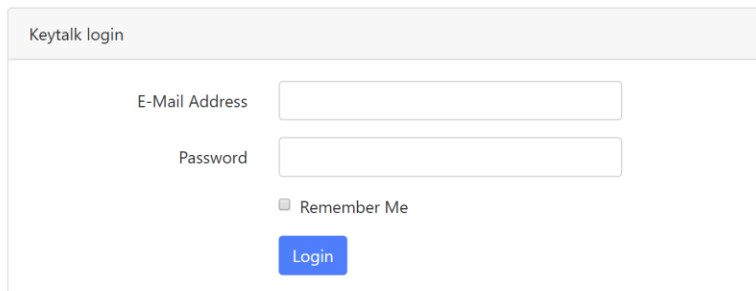
Note: An SSL trust error will happen as the virtual appliance comes with a self signed expired SSL certificate

Step 2: Access the admin GUI on:

<https://<ipaddress>:3000/login>

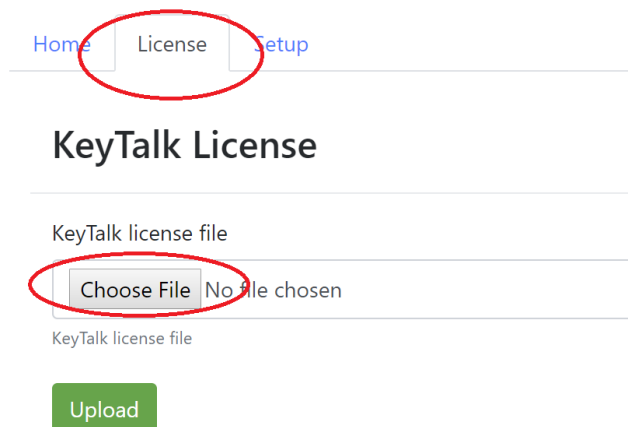
Username: <yourchosenadminusername>

Password: <yourchosenpassword>

A login form titled "Keytalk login" with a light gray header. It contains two input fields: "E-Mail Address" and "Password". Below the fields is a checkbox labeled "Remember Me" and a blue "Login" button.

Step 3: Upload your valid KeyTalk license file to activate the LDAP functionality:

SMIME LDAP HA

A screenshot of the "KeyTalk License" page. At the top, there are three tabs: "Home", "License", and "Setup". The "License" tab is selected and circled in red. Below the tabs, the title "KeyTalk License" is displayed. Underneath, there is a section titled "KeyTalk license file" which contains a file selection interface. The "Choose File" button is circled in red, and the text "No file chosen" is visible next to it. Below this section is a green "Upload" button.

Step 4: Change the LDAP HA sync password

This password is used to pull LDAP user-certificate data, and LDAP admin password from a target LDAP. Each KeyTalk LDAP comes with a default password, so not changing it will result in a party being able to clone your LDAP data.

To change it, the KeyTalk LDAP will generate a random which renews when you refresh the page. When you see a random you like, select UPDATE

Write down / cope on a secure location this password for future references, as you will need to enter the same sync password on all your KeyTalk LDAP nodes when you wish to run High Available at some point.

It will take 1-2 minutes for the sync password to change and be effectuated, wait for the text to change and the HA nodes to show at least 1 green active again.

Home License Setup

LDAP HA sync password

Security advice:
Before adding nodes to your cluster, Please change the default HA sync password. This password should be the same on ALL nodes in the cluster.

Update LDAP HA sync password:

CoMeP2LwW4xj3RafSg8z11LNxpedC80JAQ4u7D9w

Update

Customization

No custom logo setup.
Customize logo

Choose File No file chosen

Upload your own logo (Max: 100px width and/or 100px height. Filetype: PNG or GIF)

Title

Customize GUI title

Customize GUI title

Update

Step 5: Change the LDAP admin password:

This password is used to connect the KeyTalk environment to the LDAP and enable write/remove certificates to the LDAP, and is also used to manage the content of the LDAP (cluster)

Home License Setup

LDAP server settings

Admin password

New password

Confirm password

Update

Network

KeyTalk Client

Certificates

LDAP

LDAP-HA

Syslog

The LDAP Base DN is:
The LDAP Bind DN is:
The LDAP username is:
OU:

dc=keytalk,dc=com
uid=admin,dc=keytalk,dc=com
admin
People

In your KeyTalk virtual appliance the used credentials would look like:

Configure LDAP Server connection for Service Idaptest

URL: *	ldap://ldap-n1.myldapdemo.com:389 or ldaps://ldap-n1.myldapdemo.com:636	
Bind DN: *	uid=admin,dc=keytalk,dc=com	
Bind Password: *	<input type="checkbox"/> show
Allow empty password:	<input type="checkbox"/>	
Base DN: *	ou=people,dc=keytalk,dc=com	
Service User:	admin	
Service Password:	<input type="checkbox"/> show
Is Active Directory:	<input type="checkbox"/>	
Address Book only:	<input checked="" type="checkbox"/>	
Address Book DN Template: *	uid=\$(email),ou=people,dc=keytalk,dc=com	

In your ldap management software the used credentials would look like:

IMPORTANT: 636/LDAPS requires a valid FQDN matching the SAN of your SSL certificate

Connection properties

Connection name: ldap-n1.myldapdemo.com

General Options Attributes

Connection:

Host: ldap-n1.myldapdemo.com Port: 636 Version: 3

Base: dc=keytalk,dc=com

☒ Simple authentication ☐ SSL ☐ TLS
☐ GSS-API ☐ SASL

Account

Username: uid=admin,dc=keytalk,dc=com

Password:

☐ Anonymous connection

Step 6: Set the LDAP (node) FQDN hostname

For production purposes, it is important to follow this step.

For single machine Proof of Concept purposes, it is possible to skip this step and leave the hostname for what it is, and solely use the IP address, while relying on LDAP protocol only.

Contrary to what would be expected, due to High Availability functionality, changing the hostname, first requires a new DNS resolvable LDAP HA-node to be added. So ensure a DNS entry matching the FQDN exists and points to the IP of the LDAP instance you're configuring

Add the HA node based on your intended Fully Qualified Domain Name.

In this example we'll be using the FQDN: `ldapnode1.keytalk.com` and using LDAPS as the protocol (thus when a HA LDAP cluster is created, it will be enforcing secure TLS 1.2 based synchronization, instead of non-secure LDAP based cynchronization)

Home License **Setup**

Network
KeyTalk Client
Certificates
LDAP
LDAP-HA
Syslog

LDAP HA settings

2 nodes configured | **Add HA node**

No.	Host	Base	State	#
1	ldaps://ldap-n1.keytalk.com	"dc=keytalk,dc=com"		Remove
2	ldaps://ldap-n2.keytalk.com	"dc=keytalk,dc=com"		Remove

Add HA node

Ex: ldaps://node2.keytalk.com

[Close](#) **Add node**

Now update the indexes:

Home License **Setup**

Network
KeyTalk Client
Certificates
LDAP
LDAP-HA
Syslog

LDAP HA settings

3 nodes configured | **Add HA node**

No.	Host	Base	State	#
1	ldaps://ldap-n1.keytalk.com	"dc=keytalk,dc=com"		Remove
2	ldaps://ldap-n2.keytalk.com	"dc=keytalk,dc=com"		Remove
3	ldaps://ldapnode1.keytalk.com	"dc=keytalk,dc=com"		Remove

Update indexes

Remove the non-reachable (red) node and again Update the indexes

Home License **Setup**

Network
KeyTalk Client
Certificates
LDAP
LDAP-HA
Syslog

LDAP HA settings

2 nodes configured | [Add HA node](#)

No.	Host	Base	State	#
1	ldaps://ldap-n1.keytalk.com	"dc=keytalk,dc=com"		Remove
3	ldaps://ldapnode1.keytalk.com	"dc=keytalk,dc=com"		Remove

[Update indexes](#)

You'll now end-up with 2 nodes, 1 with the old hostname and 1 with the new hostname

LDAP HA settings

2 nodes configured | [Add HA node](#)

No.	Host	Base	State	#
1	ldaps://ldap-n1.keytalk.com	"dc=keytalk,dc=com"		Remove
3	ldaps://ldapnode1.keytalk.com	"dc=keytalk,dc=com"		Remove

Now change your hostname:

Home License **Setup**

Network
KeyTalk Client
Certificates
LDAP
LDAP-HA
Syslog

Network settings (ens33, 00:50:56:96:57:4b)

Machine hostname

Enter the fully qualified domainname

HTTP proxy

Enter the fully qualified domainname proxy address. Example: http://username:password@proxy.domain.com:port

Use DHCP
☒

[1.\) Save settings](#) | [2.\) Apply settings](#)

The entered hostname must match with the SSL certificate SAN DNS entry when a new SSL certificate is installed. If it doesn't match, it will not be installed.

LDAP Node HA syncing only works based on hostnames and doesn't work on IP, so ensure your hostnames are properly setup and in your DNS.

Step 7: Install an SSL certificate

For Proof of Concept this step could be skipped, enforcing LDAP protocol only.

The KeyTalk LDAP secure email address book supports certificate lookup based on HTTPS and LDAP / LDAPS

Adding an SSL certificate ensures LDAPS and HTTPS can be used, whereby LDAPS is also used for HA synching between LDAP nodes provided it is indicated in the discoverable HA node list.

KeyTalk's LDAP secure email address book, requires a KeyTalk virtual appliance to be available to obtain the SSL certificate and key.

So ensure you have your KeyTalk virtual appliance properly configured to allow for the fetching of serverauth SSL certificates, or upload a PEM or PFX manually

First upload the appropriate KeyTalk RCCD file, that links to the proper KeyTalk SERVICE under which the SSL certificate is obtained and managed.

The screenshot shows the KeyTalk web interface. At the top, there are navigation tabs: Home, License, and Setup. The Setup tab is selected and circled in red. On the left sidebar, there is a menu with items: Network, KeyTalk Client (highlighted in blue and circled in red), Certificates, LDAP, LDAP-HA, and Syslog. The main content area is titled 'KeyTalk client setup' and 'Manual'. It contains several input fields: Config name, KeyTalk API URL (FQDN) with a placeholder 'FQDN without protocol', API username, API password, Service name, and Provider name. Below these fields are two buttons: 'Update' (green) and 'Reset' (red). At the bottom, there is a section titled 'Upload RCCD file' with a label 'KeyTalk RCCD file'. Below this is a file selection area with a 'Choose File' button and the text 'No file chosen'. At the bottom of this section is a green 'Upload' button, which is circled in red.

After uploading the appropriate RCCD you need to minimally configure the required authentication data:

Home License **Setup**

Network
KeyTalk Client
Certificates
LDAP
LDAP-HA
Syslog

KeyTalk client setup

Manual

Config name
KeyTalk LDAP secure address book

KeyTalk API URL (FQDN)
keytalk.keytalk.com

API username
LDAP-NODE-1-USERNAME

API password
LDAP-NODE-1-PASSWORD

Service name
MANUAL

Provider name
KeyTalk

Update **Reset**

Either wait 5 minutes for the LDAP to automatically update the certificate, or manually enforce a renewal by pressing:

Home License **Setup**

Network
KeyTalk Client
Certificates
LDAP
LDAP-HA
Syslog

SSL Certificates

Client-side SSL authentication

CA Trust (single or chained)
Choose File No file chosen

CA Trust file
No file chosen

Common Name (CN)
Common Name (CN)

Organization (O)
Organization (O)

Organization Unit (OU)
Organization Unit (OU)

Certificate based authentication **ON**

Turn certificate based authentication ON or OFF

Current server certificate

Valid until 2019-06-24 07:45:00

Subject:
KeyTalk LDAP HA Server
Certificate
NL
KeyTalk IT Security BV
info@keytalk.com

Manual refresh
Refresh

NOTE:

KeyTalk client settings need to be configured per KeyTalk LDAP secure address Book instance.

These settings are not synched between the LDAP nodes in HA, allowing you to set different certificates and keys per node.

When all goes well, you should now see the certificate that applies to the HTTPS and LDAPS connection of your KeyTalk S/MIME LDAP secure email address book.

To figure out a potential cause if it fails, kindly check:

- a) KeyTalk AuthD log, to see if the authentication credentials might be the cause.**
- b) KeyTalk RDD log, to see if the LDAP server time might be too far off (KeyTalk server allows 1 hour difference to UTC)**
- c) KeyTalk CAD log, to see if an error might occur due to faulty certificate template settings or a problem occurring at your configured CA provider.**

NOTE: **The LDAP will auto-renew your certificate if one of the following 3 criteria are met:**

- I) The certificate was found to be revoked due to CRL**
- II) The certificate has expired**
- III) The certificate is about to expire based on the threshold time set in the KeyTalk RCCD parameters**

2.3 KeyTalk LDAP management UI: Network config

From the LDAP management UI <https://<IP>:3000/login> you can view the initially set network configuration, and apply most changes.

When making changes, to make these persistent:

- 1) save the settings**
- 2) apply the settings.**

Home License Setup

Network

KeyTalk Client

Certificates

LDAP

LDAP-HA

Syslog

Log files

Network settings (ens33, 00:0c:29:e8:04:e2)

Public hostname

ldap-n1.keytalk.com

Enter the fully qualified domainname

Machine local IP

Choose address

None public IPv4 address. Used for NAT purposes.

HTTP proxy

Proxy address. Example: http://username:password@proxy.domain.com:port

Enter the fully qualified domainname proxy address. Example: http://username:password@proxy.domain.com:port

Use DHCP

☒

1.) Save settings 2.) Apply settings

2.4 KeyTalk LDAP management UI: Admin strong authentication

From the LDAP management UI <https://<IPADDRESS>:3000/login> you can enforce strong authentication to the LDAP management UI, based on client certificate based authentication. Ensure you upload the Root and Issuing CA trust, and define the certificate subject matching criteria

Home License **Setup**

Network
KeyTalk Client
Certificates
LDAP
LDAP-HA
Syslog
Log files

SSL Certificates

Client-side SSL authentication

CA Trust (single or chained)
Choose File No file chosen
CA Trust file

Common Name (CN)
Common Name (CN)
Common Name (CN)

Organization (O)
Organization (O)
Organization (O)

Organization Unit (OU)
Organization Unit (OU)
Organization Unit (OU)

Certificate based authentication **OFF** ▼
Turn certificate based authentication ON or OFF

Update

Current server certificate

Valid until 2019-07-10 15:40:00

Subject:
KeyTalk LDAP HA Server
Certificate
NL
KeyTalk IT Security BV
info@keytalk.com

Manual refresh

KeyTalk Client based manual refresh

Should you accidentally misconfigure this and create a lockout, then you can use the CLI menu to reset the machine back to username/password authentication, using option 11

```
1) Show IP info
2) Setup network
3) Show running processes
4) Show blacklist
5) Reset to factory defaults
6) Set shell password
7) Reset Web-GUI password
8) Reset Firewall
9) Disable Firewall
10) Start Firewall
11) Disable client side SSL authentication
12) Refresh certificate
13) Show webserver log
14) Show system log
15) Configure syslog server
16) Update
17) Quit
Please enter your choice:
```

2.5 KeyTalk LDAP management UI: High Availability

The KeyTalk LDAP supports a High Availability configuration, whereby each LDAP node uses native LDAP functionality to sync LDAP data to the other known LDAP nodes.

The data that gets synched is directly related to LDAP, this includes solely:

- ✓ LDAP (write/change) admin account password
- ✓ Stored accounts and corresponding S/MIME certificates
- ✓ Status (sync) indexes

As a result for each LDAP node, you have to individually configure:

- The web management admin username/password
- Certificate based strong authentication for the management interface
- Networking (IP, DNS, proxy etc)
- KeyTalk Client settings to fetch the SSL certificate
- Syslogserver
- HTTPS lookup title
- HTTPS lookup logo

LDAP is a pretty strict protocol and complex when it comes to configuring it properly for HA.

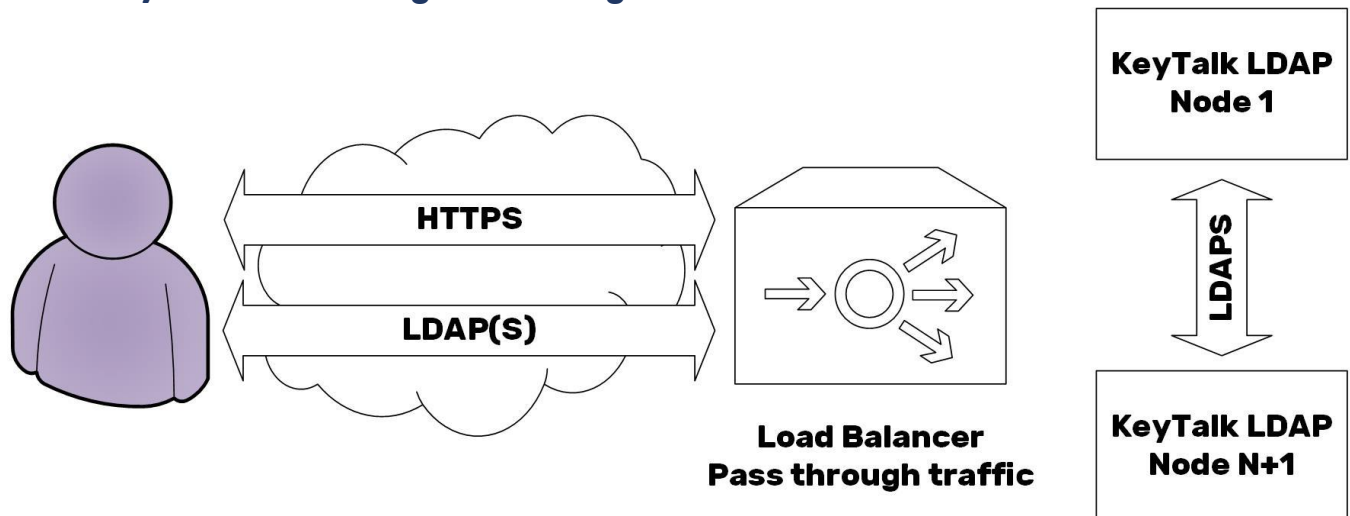
The KeyTalk LDAP management UI enables fairly easy configuration of this complex configuration process, provided the below steps are followed properly.

Not following these steps properly will likely result in the LDAP node to get corrupted, requiring it to be reinstalled or restored from a snapshot.

Before starting HA configuration ensure you have a snapshot or backup in case something goes wrong.

NOTE: At least 2 LDAP nodes must always be present in the KeyTalk S/MIME LDAP secure email address book, even if they are not all being used or are reachable (red).

2.5.1 KeyTalk LDAP HA high over design



2.5.2 KeyTalk HA configuration

Thoroughly read all required steps first, as you may have performed some already as per the quick guide steps

Step 1: FIRST ensure your HA sync password is set correctly and is the same for each LDAP node. Do NOT use the default sync password for production purposes!

Home License Setup

LDAP HA sync password

Security advice:
Before adding nodes to your cluster; Please change the default HA sync password. This password should be the same on ALL nodes in the cluster.

Update LDAP HA sync password:

CoMeP2LwW4xj3RafSg8z11LNxpedC80JAQ4u7D9w

Update

Step 2: Add the FQDN as a new HA node which represents this machine. Ensure that either ldaps:// or ldaps:// is used, ie the trusted SSL certificate must be installed or ldaps won't work.

Home License Setup

LDAP HA settings

2 nodes configured | Add HA node

No.	Host	Base	State	#
1	ldaps://ldap-n1.keytalk.com	"dc=keytalk,dc=com"		Remove
2	ldaps://ldap-n2.keytalk.com	"dc=keytalk,dc=com"		Remove

Add HA node

ldaps://dapnode1.keytalk.com

Ex: ldaps://node2.keytalk.com

Close Add node

Step 3: Update the indexes:

Home License Setup

LDAP HA settings

3 nodes configured | Add HA node

No.	Host	Base	State	#
1	ldaps://ldap-n1.keytalk.com	"dc=keytalk,dc=com"		Remove
2	ldaps://ldap-n2.keytalk.com	"dc=keytalk,dc=com"		Remove
3	ldaps://dapnode1.keytalk.com	"dc=keytalk,dc=com"		Remove

Update indexes

Step 4: Remove the non-reachable (red) node and again update the indexes

Home License **Setup**

Network
KeyTalk Client
Certificates
LDAP
LDAP-HA
Syslog

LDAP HA settings

2 nodes configured | [Add HA node](#)

No.	Host	Base	State	#
1	ldaps://ldap-n1.keytalk.com	"dc=keytalk,dc=com"	■	Remove
3	ldaps://ldapnode1.keytalk.com	"dc=keytalk,dc=com"	■	Remove

[Update indexes](#)

Step 5: Change your hostname:

Home License **Setup**

Network
KeyTalk Client
Certificates
LDAP
LDAP-HA
Syslog

Network settings (ens33, 00:50:56:96:57:4b)

Machine hostname

Enter the fully qualified domainname

HTTP proxy

Enter the fully qualified domainname proxy address. Example: http://username:password@proxy.domain.com:port

Use DHCP
☒

[1.\) Save settings](#) [2.\) Apply settings](#)

Step 6: Set the KeyTalk client details enabling the fetching of the SSL certificate to support LDAPS

First upload the appropriate KeyTalk RCCD file, that links to the proper KeyTalk SERVICE under which the SSL certificate is obtained and managed.

Home License **Setup**

Network
KeyTalk Client
Certificates
LDAP
LDAP-HA
Syslog

KeyTalk client setup

Manual

Config name

KeyTalk API URL (FQDN)

API username

API password

Service name

Provider name

Upload RCCD file

KeyTalk RCCD file
 No file chosen

After uploading the appropriate RCCD you need to minimally configure the required authentication data:

Home License **Setup**

Network
KeyTalk Client
Certificates
LDAP
LDAP-HA
Syslog

KeyTalk client setup

Manual

Config name

KeyTalk API URL (FQDN)

API username

API password

Service name

Provider name

Step 7: Install the SSL certificate

Either wait 5 minutes for the LDAP to automatically update the certificate, or manually enforce a renewal by pressing REFRESH when using the KeyTalk CLM to issue the LDAP server certificate:

Home License **Setup**

Network
KeyTalk Client
Certificates
LDAP
LDAP-HA
Syslog

SSL Certificates

Client-side SSL authentication

CA Trust (single or chained)
 No file chosen

CA Trust file
Common Name (CN)

Common Name (CN)

Organization (O)

Organization (O)

Organization Unit (OU)

Organization Unit (OU)

Certificate based authentication ☒ ON
Turn certificate based authentication ON or OFF

Current server certificate

Valid until 2019-06-24 07:45:00

Subject:
KeyTalk LDAP HA Server
Certificate
NL
KeyTalk IT Security BV
info@keytalk.com

Manual refresh

NOTE: **KeyTalk client settings need to be configured per KeyTalk LDAP secure address Book instance.**

These settings are not synched between the LDAP nodes in HA, allowing you to set different certificates and keys per node.

Alternatively manually upload your LDAP certificate and key:

Home License **Setup**

Network
KeyTalk Client
Certificates
LDAP
LDAP-HA
Syslog
Log files

SSL Certificates

Custom certificate and private key

Server Certificate PFX
 No file chosen

Certificate + trust chain in PFX

PFX Password

PFX export password

-- OR --

Server Certificate (PEM) + trust chain
 No file chosen

Certificate + trust chain

Certificate Private Key
 No file chosen

Private Key

Step 8: Wait until you see that the certificate is renewed successfully or got uploaded successfully

Step 9: Follow the same steps 1-8 for each KeyTalk LDAP node you are deploying

Step 10: Add each deployed and configured node to each other and update the indexes with each entry

Home License **Setup**

Network
KeyTalk Client
Certificates
LDAP
LDAP-HA
Syslog

LDAP HA settings

2 nodes configured **Add HA node**

No.	Host	Base	State	#
1	ldaps://ldap-n1.keytalk.com	"dc=keytalk,dc=com"		Remove
3	ldaps://ldapnode1.keytalk.com	"dc=keytalk,dc=com"		Remove

Add HA node ×

ldaps://ldapnode2.keytalk.com
Ex: ldaps://node2.keytalk.com

[Close](#) **Add node**

Home License **Setup**

Network
KeyTalk Client
Certificates
LDAP
LDAP-HA
Syslog

LDAP HA settings

3 nodes configured | **Add HA node**

No.	Host	Base	State	#
1	ldaps://ldap-n1.keytalk.com	"dc=keytalk,dc=com"		Remove
3	ldaps://ldapnode1.keytalk.com	"dc=keytalk,dc=com"		Remove
4	ldaps://ldapnode2.keytalk.com	"dc=keytalk,dc=com"		Remove

Update indexes

NOTE: The state of each node is show in:

Green: The node is discoverable, the connection is trusted and the sync keys match

Red: The target node's FQDN cannot be resolved, or the LDAPDS SSL certificate is not trusted, or the sync key is mismatching, or the machine is simply unreachable

A REST API call can be used to remotely monitor the status of each LDAP node:

<https://<url>/api/ldap/node/status/<index ID>>

3 S/MIME LDAP secure email address book content

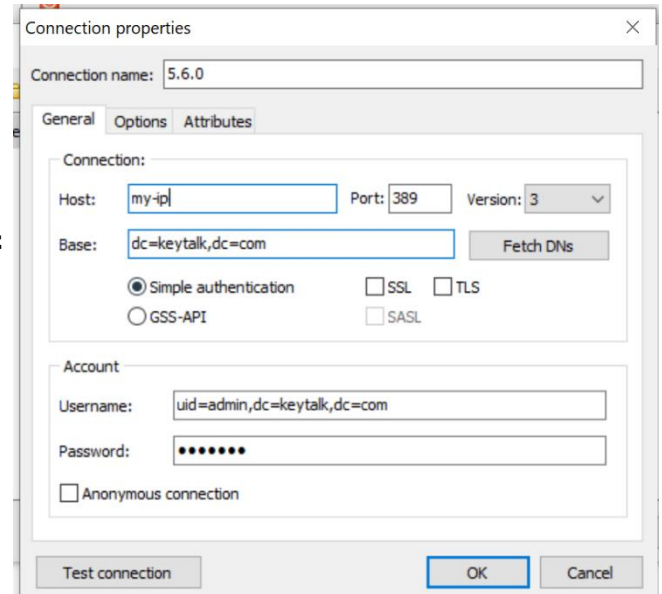
3.1 Directly accessing the LDAP for management

Under KeyTalk SERVICES an appropriate KeyTalk Admin can set the LDAP S/MIME server address-book details, so a future version of Plenty of LDAP management tools exist. KeyTalk customers mostly use: <http://www.ldapadmin.org/download/ldapadmin.html>

As the connection settings use your network details:

Base: dc=keytalk,dc=com
Username: uid=admin,dc=keytalk,dc=com
Password: <yoursetpassword>

IMPORTANT: Using 636/LDAPS requires a valid host FQDN as part of your SSL certificate SAN



3.2 Writing KeyTalk managed certificates to the LDAP

In the KeyTalk virtual appliance management UI, ensure that you have setup a SERVICE capable of issuing client certificates with appropriate S/MIME support (email protection).

Connect an LDAP authentication module to the SERVICE, either as a primary LDAP, or secondary in addition to for example your Active Directory.

Ensure the following settings are used in your KeyTalk LDAP Authentication module (mind the Address Book only checkmark!): Configure LDAP Server connection for Service ldap

URL: *	ldap://<your-ip>:389 or ldaps://<your-ip>:636	i
Bind DN: *	uid=admin,dc=keytalk,dc=com	i
Bind Password: *	<Yoursetpassword>	show i
Allow empty password:	<input type="checkbox"/>	i
Base DN: *	ou=people,dc=keytalk,dc=com	
Service User:	admin	i
Service Password:	<Yoursetpassword>	show
Is Active Directory:	<input type="checkbox"/>	
Address Book only:	<input checked="" type="checkbox"/>	i
Address Book DN Template: *	uid=\$(email),ou=people,dc=keytalk,dc=com	i



Invalid LDAP bind attempts are considered as if invalid credentials were supplied by the KeyTalk user, provided the LDAP server is physically accessible



It is recommended to verify the entered Bind DN and Bind Password using the "CHECK" button.

OK CHECK CANCEL

LDAPS CA Certificate *No Certificate Found*

3.3 Writing non-KeyTalk managed certificates to the LDAP

When you do not wish to make use of the KeyTalk Certificate Life Cycle Management (CLM) virtual appliance, you can also opt to write your certificates directly into the LDAP using the LDAP protocol. The following would need to be used in addition to your set LDAP admin password:

DN, CN, SN, objectClass, mail and userCertificate

Used DN: "uid={emailaddress},{baseDN}"

OU=people, DC=keytalk, DC=com

3.4 Restoring KeyTalk managed certificates to the LDAP

Should you ever lose the content of your KeyTalk S/MIME LDAP secure address book, then you can easily restore the content directly from the KeyTalk Certificate Life Cycle Management (CLM) virtual appliance.

Simply access your KeyTalk management UI, and select the DEVID USERS group of lost certificates you wish to populate again in the LDAP :

The screenshot shows the KeyTalk management UI with the 'DEVID USERS' tab selected. The 'View & Edit' link is circled in red. Below the tab, the 'Service' dropdown is set to 'test' and circled in red. The 'User Name' field is empty. The 'In Learn Mode' dropdown is set to '--any--'. The 'Having at least one Slot' checkbox is checked. The 'with Hardware Signature' checkbox is checked. The 'Results Per Page' dropdown is set to '10'. The 'SEARCH' button is circled in red.

Now select:

Click "Revoke" to revoke certificates of **all found users**.

REVOKE

Click "Enroll" to request a certificate for **each found user** without a valid certificate.

ENROLL

Click "Store Certs to LDAP" to re-submit all valid certificates for **each found user** to LDAP.

STORE CERTS TO LDAP

Click "Export CSV" to export **all found users** to CSV.

EXPORT CSV

Click "Close Slots" to close (lock) learn-once slots and cancel slot auto-closing timers of **all found users**.

CLOSE SLOTS

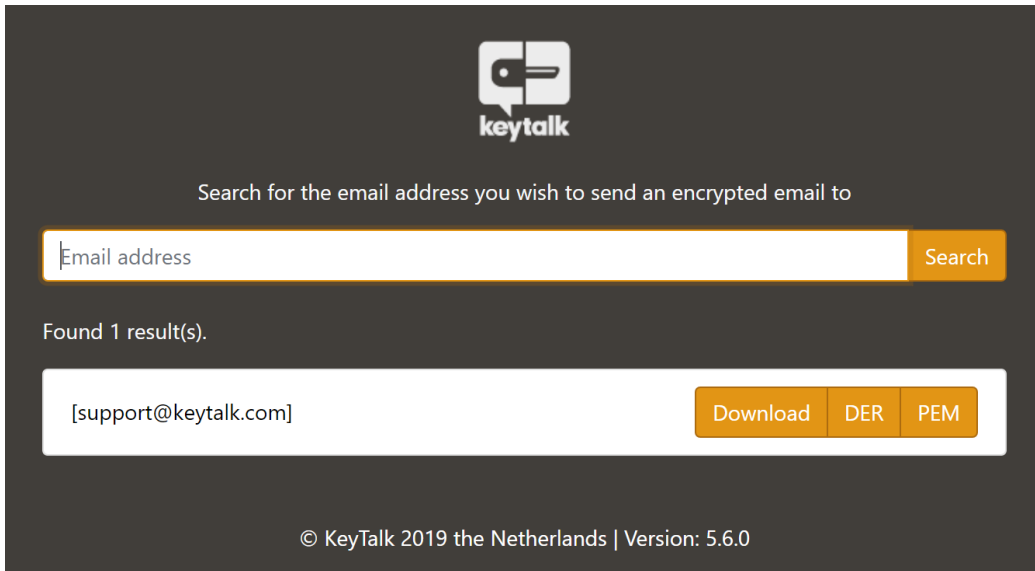
4 KeyTalk S/MIME LDAP as a web and mail client address book

4.1 Web based S/MIME email address book lookup

The LDAP web-interface listens by default on <https://<sethostname>>

In order to properly use <https://<setipaddress>> a valid SSL certificate is required. See chapter 1.2 step 6.

The HTTPS based S/MIME address search allows for exact match only lookups for email address S/MIME public key and certificate information in PEM/CRT and DER format. Wildcards are not permitted.



The screenshot shows the KeyTalk web interface. At the top is the KeyTalk logo. Below it is a search bar with the placeholder text "Email address" and a "Search" button. Below the search bar, it says "Found 1 result(s)." and displays the email address "[support@keytalk.com]". To the right of the email address are three buttons: "Download", "DER", and "PEM". At the bottom, it says "© KeyTalk 2019 the Netherlands | Version: 5.6.0".

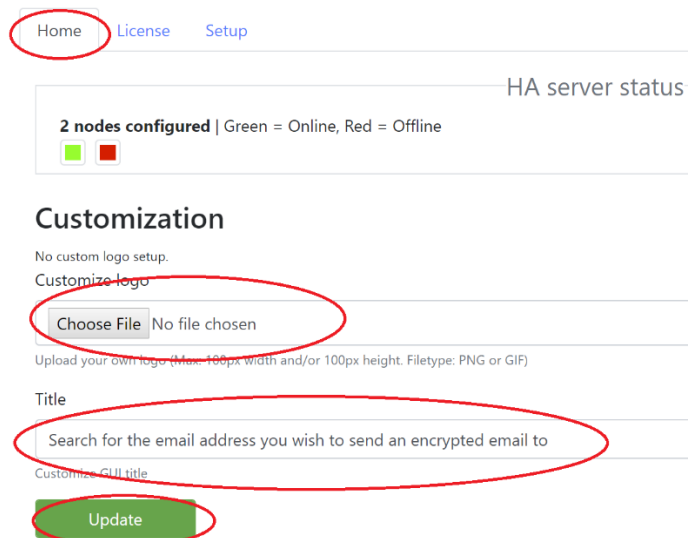
4.1 Webbased lookup basic look and feel change

The KeyTalk HTTPS based lookup of S/MIME secure email certificates supports basic look and feel changes, allowing changes to the logo and changes to the title.

Color and font type changes are not supported in this release.

The custom logo must be 100x100 pixels in PNG or in GIF (animated gif is also supported)

The title supports UTF8 character sets, and can have a maximum length of 250 characters. URL links are shown as plain text only to prevent potential abuse.



The screenshot shows the KeyTalk web interface with the "Home" link circled in red. Below the navigation bar is a section titled "HA server status" showing "2 nodes configured" with a legend: Green = Online, Red = Offline. Below this is a "Customization" section. It has a "Customize logo" section with a "Choose File" button and "No file chosen" text. Below that is a "Title" section with a text input field containing "Search for the email address you wish to send an encrypted email to". At the bottom is an "Update" button circled in red.

4.2 Mail client based S/MIME email address book lookup

The LDAP listens by default on [ldap://<sethostname>](#) using port 389

In order to properly use [ldaps://<sethostname>](#) or [ldaps://<setipaddress>](#) on port 636, a valid SSL certificate is required. See chapter 1.2 step 11.

The LDAP(S) based S/MIME address search allows for a single return of a matching email address value only

4.2.1 Automated mail client address book configuration

As of KeyTalk client and virtual appliance 5.5.5, the KeyTalk solution supports automated LDAP address book configuration for Outlook and MacMail on Windows and Mac.

Under KeyTalk SERVICES an appropriate KeyTalk Admin can set the LDAP S/MIME server address-book details, the KeyTalk client can auto-configure the supported mail client, by means an inbuilt REST-API fetch of these details.

Up to 3 different address books can be configured to be pushed automatically for auto configuration.

Set the LDAP address book in the KeyTalk virtual appliance under the appropriate SERVICE :

LDAP/AD Settings

LDAP/AD Settings

Allow Enrolling S/MIME Certificates to External Parties: ☐

Install secure email S/MIME certificate to LDAP: ☒

Update Alt-Security-Identities in LDAP: ☐

LDAP URL:

Search Base:

Public LDAP Address Books:

LDAP URL:

Search Base:

LDAP URL:

Search Base:

Apply Address Books: ☒

Now as soon as someone authenticates positively using the KeyTalk client, the address book is configured for either Outlook or MacMail or both when applicable.

Thunderbird is currently not covered. Should you have a need for it to be supported, kindly let us know.

4.2.2 Manual mail client address book configuration

You can configure this LDAP as your mailclient's address book, by adding it manually to your mailclient.
Example in Outlook:

Account Settings

Directories and Address Books

You can choose a directory or address book below to change or remove it.

Email Data Files RSS Feeds SharePoint Lists Internet Calendars Published Calendar Address Books

New... Change... Remove

Name	Type
Outlook Address Book	MAPI
smime.keytalk.com	LDAP

Microsoft LDAP Directory

Connection Search

Server Settings

Search timeout in seconds: 60

Specify the maximum number of entries you want to return after a successful search: 100

Search Base

☐ Use Default

☒ Custom: ou=People,dc=keytalk,dc=com

Browsing

☐ Enable Browsing (requires server support)

OK Cancel Apply

More Settings...

5 KeyTalk contact details and 3rd line support

**KeyTalk IT Security is registered with the Dutch chamber of commerce under: 59072555
with registered VAT number: NL853305766B01**

**Our office address:
New Day Office
KeyTalk IT Security
Maanlander 47
3824MN Amersfoort
The Netherlands**

**Phone: +31 88 KEYTALK or +31 88 5398255
Email: [sales\[at\]keytalk.com](mailto:sales[at]keytalk.com)
Opening hours: Mo-Fr 08:00 – 18:00**

**Customer and partner technical 3rd line support
Phone: +31 88 KEYTALK or +31 88 5398255
Email: [support\[at\]keytalk.com](mailto:support[at]keytalk.com)
Opening hours: Mo-Su 00:00 – 24:00 (24/7)**

**Website: <https://www.keytalk.com>
Firmware/software: <https://www.keytalk.com/download>**

ANNEX A: Importing KeyTalk LDAP virtual appliance in AWS

AWS online guides include:

<https://aws.amazon.com/ec2/vm-import/>

<https://docs.aws.amazon.com/vm-import/latest/userguide/vm-import-ug.pdf>

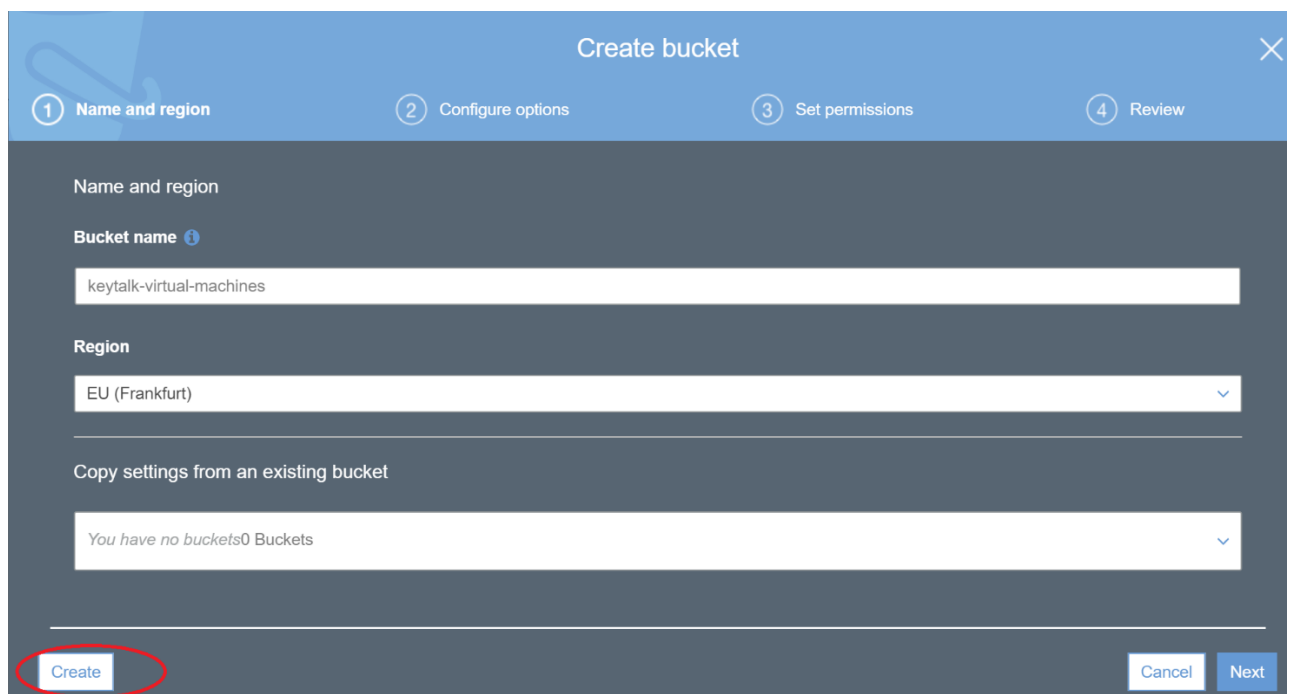
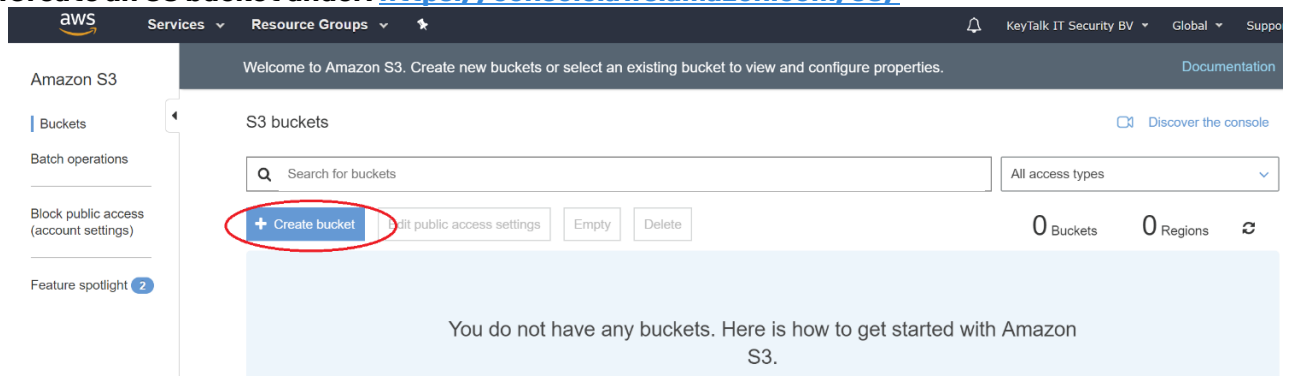
The below guide is a summary of the links above enhanced with hands-on experience.

This guide assumes that you have already created an account for AWS and configured payment for it.

Step 1: Ensure you have downloaded the KeyTalk S/MIME LDAP secure email address book for AWS/VMware

Step 2: Login to AWS <https://aws.amazon.com/console/>

Step 3: Create an S3 bucket under: <https://console.aws.amazon.com/s3/>



Step 4: Enable public access to the KeyTalk S3 bucket.

Since KeyTalk virtual appliances are public anyhow, this does not affect your security.

However if this is an issue, feel free to close public access to the S3 bucket after importing the virtual machine into EC2 at the end of this guide.

S3 buckets Discover the console

Search for buckets All access types

[+ Create bucket](#) [Edit public access settings](#) [Empty](#) [Delete](#)

1 Buckets 1 Regions [Refresh](#)

<input checked="" type="checkbox"/>	Bucket name	Access	Region	Date created
<input checked="" type="checkbox"/>	keytalk-virtual-machines	Objects can be public	EU (Frankfurt)	Jun 10, 2019 7:15:03 PM GMT+0200

Edit block public access settings for selected buckets

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, or both. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block *all* public access. These settings apply only to selected buckets. AWS recommends that you turn on Block *all* public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

- ☒ **Block *all* public access**
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.
 - ☒ **Block public access to buckets and objects granted through *new* access control lists (ACLs)**
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
 - ☒ **Block public access to buckets and objects granted through *any* access control lists (ACLs)**
S3 will ignore all ACLs that grant public access to buckets and objects.
 - ☒ **Block public access to buckets and objects granted through *new* public bucket policies**
S3 will block new bucket policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
 - ☒ **Block public and cross-account access to buckets and objects through *any* public bucket policies**
S3 will ignore public and cross-account access for buckets with policies that grant public access to buckets and objects.

[Cancel](#) [Save](#)

Step 5: Select the created bucket and upload your KeyTalk LDAP secure email address book virtual appliance whereby you minimally upload the included VMDK file:

Amazon S3 > keytalk-virtual-machines

Overview **Properties** Permissions Management

[Upload](#) [+ Create folder](#) [Download](#) [Actions](#)

While most customers choose the Standard storage class, kindly read about storage classes and ensure you choose the class that best fits your scenario!

Upload

Select files

Set permissions

3 Set properties

4 Review

2 Files Size: 5.3 GB Target path: keytalk-virtual-machines

Storage class

Choose a storage class based on your use case and access requirements. [Learn more](#) or see [Amazon S3 pricing](#)

Storage class	Designed for	Availability Zones	Min storage duration	Min billable object size	Monitoring and automation fees	Retrieval fees
<input type="radio"/> Standard	Frequently accessed data	≥ 3	-	-	-	-
<input type="radio"/> Intelligent-Tiering	Long-lived data with changing or unknown access patterns	≥ 3	30 days	-	Per-object fees apply	-
<input type="radio"/> Standard-IA	Long-lived, infrequently accessed data	≥ 3	30 days	128KB	-	Per-GB fees apply
<input type="radio"/> One Zone-IA	Long-lived, infrequently accessed, non-critical data	≥ 1	30 days	128KB	-	Per-GB fees apply

Upload

Previous

Next

Upload

Select files

Set permissions

Set properties

4 Review

Files

2 Files Size: 5.3 GB

Permissions

1 grantees

Properties

Encryption
No

Storage class
Standard

Metadata
Tag

Previous

Upload

Amazon S3 > keytalk-virtual-machines

Overview

Properties

PermissionsPublic

Management

Q

Type a prefix and press Enter to search. Press ESC to clear.

Upload

Create folder

Download

Actions

EU (Frankfurt)

Viewing 1 to 2

<input type="checkbox"/>	Name	Last modified	Size	Storage class
<input type="checkbox"/>	disk-0.vmdk	Oct 2, 2019 2:39:40 AM GMT+0200	1015.7 MB	Standard

Step 6: Lookup and note down the VMDK Object url.
Select the vmdk file and open the OVERVIEW tab:

The screenshot shows the AWS S3 console interface. At the top, there are four tabs: Overview, Properties, Permissions, and Select from. The Overview tab is selected and circled in red. Below the tabs, there are five buttons: Open, Download, Download as, Make public, and Copy path. The main content area displays the following information:

- Owner:** f7d70c62712f5d3afea46c44a610da093a590b293b3426576cdadd8da3e9c9ad
- Last modified:** Oct 2, 2019 2:39:40 AM GMT+0200
- Etag:** 509f092681b9e90e36fbb7f4546faaf2-62
- Storage class:** Standard
- Server-side encryption:** None
- Size:** 1015.7 MB
- Key:** disk-0.vmdk
- Object URL:** <https://keytalk-virtual-machines.s3.eu-central-1.amazonaws.com/disk-0.vmdk> (This URL is circled in red)

Step 7: Create an AWS administrator IAM user under:

<https://console.aws.amazon.com/iam/>

Follow these steps:

https://docs.aws.amazon.com/IAM/latest/UserGuide/getting-started_create-admin-group.html

Step 8: Create and remember the AWS administrator IAM user Access key:

- **Select the created user**
- **Select the Security credentials tab**

The screenshot shows the AWS IAM console interface. On the left, there is a navigation menu with options: Dashboard, Groups, Users, Roles, Policies, Identity providers, Account settings, Credential report, and Encryption keys. The Users option is circled in red. The main content area shows the 'Security credentials' tab for a selected user. The tab is circled in red. The 'Sign-in credentials' section shows a summary of the user's sign-in information. The 'Access keys' section shows a 'Create access key' button, which is circled in red. Below this, there is a table with columns: Access key ID, Created, Last used, and Status. The table is currently empty, showing 'No results'.

Step 9: Install the AWS CLI:

<https://docs.aws.amazon.com/cli/latest/userguide/cli-chap-install.html#install-tool-bundled>

Step 10: Create an AWS CLI userprofile, from your local machine console type:

aws configure

Enter the requested details, in our example the following applies:

```
C:\WINDOWS\system32>aws configure
AWS Access Key ID [None]: AKI 73
AWS Secret Access Key [None]: Sq Lk
Default region name [None]: eu-central-1
Default output format [None]: json
```

Lookup your region using the following reference table:

<https://docs.aws.amazon.com/general/latest/gr/rande.html>

Step 11: Create a containers.json file in the directory you are running the aws command from, with the following content matching your chosen settings and most important the vmdk Object url:

```
[
{
  "Description": "KeyTalk SMIME LDAP",
  "Format": "vmdk",
  "Url": "https://keytalk-virtual-machines.s3.eu-central-1.amazonaws.com/disk-0.vmdk"
}
]
```

Step 12: Import the VMDK as an Amazon Machine Image (AMI) using the following command:

```
aws ec2 import-image --description "KeyTalk LDAP VMDK" --disk-containers
"file://containers.json"
```

The following returned value is expected:

```
C:\aws>aws ec2 import-image --description "KeyTalk LDAP VMDK" --disk-containers "file://containers.json"
{
  "Description": "KeyTalk LDAP VMDK",
  "ImportTaskId": "import-ami-0679a1beb187b5277",
  "Progress": "2",
  "SnapshotDetails": [
    {
      "DiskImageSize": 0.0,
      "Format": "VMDK",
      "Url": "https://keytalk-virtual-machines.s3.eu-central-1.amazonaws.com/disk-0.vmdk"
    }
  ],
  "Status": "active",
  "StatusMessage": "pending"
}
```

C:\aws>

Step 13: Verify the status of the import using the following command:

```
aws ec2 describe-import-image-tasks --import-task-ids import-ami-<my-ami-ID>
```

given the above example the command is:

```
aws ec2 describe-import-image-tasks --import-task-ids import-ami-0679a1beb187b5277
```

When the task is complete you should see a Completed status similar to:

```
C:\aws>aws ec2 describe-import-image-tasks --import-task-ids import-ami-0679a1beb187b5277
{
  "ImportImageTasks": [
    {
      "Architecture": "x86_64",
      "Description": "KeyTalk LDAP VMDK",
      "ImageId": "ami-0f06e3e39d451fa6f",
      "ImportTaskId": "import-ami-0679a1beb187b5277",
      "LicenseType": "BYOL",
      "Platform": "Linux",
      "SnapshotDetails": [
        {
          "Description": "KeyTalk SMIME LDAP",
          "DeviceName": "/dev/sda1",
          "DiskImageSize": 1065027072.0,
          "Format": "VMDK",
          "SnapshotId": "snap-0bad813f04bf701db",
          "Status": "completed",
          "Url": "https://keytalk-virtual-machines.s3.eu-central-1.amazonaws.com/disk-0.vmdk",
          "UserBucket": {}
        }
      ],
      "Status": "completed"
    }
  ]
}
```

Step 14: Launch your created Amazon Machine Instance (AMI) as an EC2 Instance for your AWS region:

The screenshot shows the AWS Management Console interface. On the left, the 'EC2 Dashboard' is selected in the navigation menu. The main area displays 'Resources' for the EU Central (Frankfurt) region, including 1 Running Instance, 0 Elastic IPs, 2 Snapshots, 2 Volumes, 0 Load Balancers, 0 Key Pairs, 3 Security Groups, 0 Dedicated Hosts, and 0 Placement Groups. Below this, there's a 'Create Instance' section with a 'Launch Instance' button circled in red. A 'Service Health' section shows 'EU Central (Frankfurt)' with a green status icon. A 'Scheduled Events' section shows 'No events'.

Step 1: Choose an Amazon Machine Image (AMI)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

The screenshot shows the 'Choose an Amazon Machine Image (AMI)' page. The 'My AMIs' tab is selected and circled in red. Two AMIs are listed: 'import-ami-0040e2de2048a5385' and 'import-ami-0679a1beb187b5277'. The second AMI is circled in red, and its 'Select' button is also circled in red. The page includes a search bar at the top and a 'Quick Start' section on the left.

Depending on your performance requirement, select an Instance Type that offers at least 2 cores and 4 Gb memory (t2.medium / t3.medium), preferably 4 cores and 8 Gb memory (t2.xlarge / t3.xlarge)

Step 2: Choose an Instance Type

<input type="checkbox"/>	General purpose	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.large	2	8	EBS only	-	Low to Moderate	Yes
<input checked="" type="checkbox"/>	General purpose	t2.xlarge	4	16	EBS only	-	Moderate	Yes
<input type="checkbox"/>	General purpose	t2.2xlarge	8	32	EBS only	-	Moderate	Yes
<input type="checkbox"/>	General purpose	t3.nano	2	0.5	EBS only	Yes	Up to 5 Gigabit	Yes
<input type="checkbox"/>	General purpose	t3.micro	2	1	EBS only	Yes	Up to 5 Gigabit	Yes
<input type="checkbox"/>	General purpose	t3.small	2	2	EBS only	Yes	Up to 5 Gigabit	Yes
<input type="checkbox"/>	General purpose	t3.medium	2	4	EBS only	Yes	Up to 5 Gigabit	Yes
<input type="checkbox"/>	General purpose	t3.large	2	8	EBS only	Yes	Up to 5 Gigabit	Yes
<input type="checkbox"/>	General purpose	t3.xlarge	4	16	EBS only	Yes	Up to 5 Gigabit	Yes
<input type="checkbox"/>	General purpose	t3.2xlarge	8	32	EBS only	Yes	Up to 5 Gigabit	Yes

Cancel Previous **Review and Launch** Next: Configure Instance Details

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 7: Review Instance Launch

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

AMI Details

 **import-ami-0679a1beb187b5277 - ami-0f06e3e39d451fa6f**
 AWS-VMImport service: Linux - CentOS Linux release 7.6.1810 (Core) - 3.10.0-957.5.1.el7.x86_64
 Root Device Type: ebs Virtualization type: hvm

[Edit AMI](#)

Instance Type

[Edit instance type](#)

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
t2.medium	Variable	2	4	EBS only	-	Low to Moderate

Security Groups

[Edit security groups](#)

Security group name launch-wizard-2
Description launch-wizard-2 created 2019-10-02T03:05:01.524+02:00

Type	Protocol	Port Range	Source	Description
------	----------	------------	--------	-------------

Cancel Previous **Launch**

Select an existing key pair or create a new key pair



A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about [removing existing key pairs from a public AMI](#).

Proceed without a key pair

☒ I acknowledge that I will not be able to connect to this instance unless I already know the password built into this AMI.

Cancel **Launch Instances**

Possibly the instance will not launch as your account first needs a verification by AWS based on your chosen region.

Step 15: Set the Security policy firewall rules and inbound ports
Go to EC2 Security Groups, and select either edit existing or create new:

The screenshot shows the AWS Management Console interface. In the left-hand navigation menu, under the 'NETWORK & SECURITY' section, the 'Security Groups' link is highlighted with a red circle. Above it, the 'Create Security Group' button is also highlighted with a red circle. The main content area shows a table of existing security groups with columns: Name, Group ID, Group Name, VPC ID, Owner, and Description. One group is listed: 'default' with Group ID 'sg-37c76157' and VPC ID 'vpc-94afb3ff'.

Create Security Group

Security group name

Description

VPC

Security group rules:

Type	Protocol	Port Range	Destination	Description
All traffic	All	0 - 65535	Custom 0.0.0.0/0	e.g. SSH for Admin C

Create Security Group

Security group name

Description

VPC

Security group rules:

Type	Protocol	Port Range	Source	Description
Custom TCP F	TCP	443	Custom 0.0.0.0/0, ::/0	e.g. SSH for Admin
Custom TCP F	TCP	389	Custom 0.0.0.0/0, ::/0	e.g. SSH for Admin
Custom TCP F	TCP	636	Custom 0.0.0.0/0, ::/0	e.g. SSH for Admin
Custom TCP F	TCP	3000	Custom 0.0.0.0/0, ::/0	e.g. SSH for Admin

Step 16: Apply the security group:

Select the KeyTalk LDAP secure email address book from EC2 and select:

The screenshot shows the AWS Management Console interface. On the left, the 'INSTANCES' menu is expanded, and 'Instances' is selected. In the main area, the 'Actions' dropdown menu is open, and 'Networking' is selected. Within the 'Networking' submenu, 'Change Security Groups' is highlighted. The instance details for 'i-065843c093132a596' are visible, showing it is running in the eu-central-1 availability zone with a public IP of 18.196.163.212.

Assign the security group and confirm:

Change Security Groups

Instance ID: i-065843c093132a596

Interface ID: eni-0826580ec21306cb4

Select Security Group(s) to associate with your instance

	Security Group ID	Security Group Name	Description
<input type="checkbox"/>	sg-37c76157	default	default VPC security group
<input type="checkbox"/>	sg-0d8524a1028beb26d	KeyTalk Server	KeyTalk Server FW rules
<input type="checkbox"/>	sg-095c30968de9d07e3	launch-wizard-1	launch-wizard-1 created 2019-10-02T02:08:27.426+02:00
<input type="checkbox"/>	sg-09975d7c9c9cfa4d0	launch-wizard-2	launch-wizard-2 created 2019-10-02T03:05:01.524+02:00
<input checked="" type="checkbox"/>	sg-0a457abac48f7c56d	SMIME-LDAP	KeyTalk SMIME LDAP Address Book

[Cancel](#) [Assign Security Groups](#)

Step 17: Lookup the IP address and register your account using port :3000/register over HTTPS:

The screenshot shows the AWS Management Console interface. On the left, the 'INSTANCES' menu is expanded, and 'Instances' is selected. In the main area, the details for instance 'i-065843c093132a596' are displayed. The 'Public DNS (IPv4)' is 'ec2-18-196-163-212.eu-central-1.compute.amazonaws.com' and the 'IPv4 Public IP' is '18.196.163.212'. The instance is running in the eu-central-1 availability zone.

ANNEX B: Importing KeyTalk LDAP virtual appliance in Azure

Step 1: Download the KeyTalk virtual appliance for Hyper-V / Azure from the KeyTalk website download section.

OR use the pre-uploaded public available Azure Blob as found here:

<https://keytalkvirtualappliances.blob.core.windows.net/keytalk-virtual-appliance-565/LDAP-HA-VHD.vhd>

and continue with step 4

Step 2: Go to: <https://portal.azure.com/#home>

Step 3: Go to: Storage accounts -> select your general purpose storage account -> select your container under blobs

Now upload the KeyTalk VHD to your container as a "Page Blob" as set under "advanced"

Upload blob
keytalk-virtual-appliance-565/

Files ⓘ
"LDAP-HA-VHD.vhd"

☐ Overwrite if files already exist

^ Advanced

Authentication type ⓘ
Azure AD user account **Account key**

Blob type ⓘ
Page blob

☒ Upload .vhd files as page blobs (recommended)

Block size ⓘ
4 MB

Upload to folder

Upload

Step 4: After the upload go to Azure Portal -> Disks -> ADD and select the uploaded VHD

* Subscription ⓘ Pay-as-you-go

* Resource group ⓘ KeyTalk_Virtual_Appliances
[Create new](#)

Disk details

* Disk name ⓘ KeyTalk_SMIME_LDAP_HA ✓

* Region ⓘ (Europe) West Europe

Availability zone None

Source type ⓘ Storage blob

Source subscription Pay-as-you-go

* Source blob ⓘ <https://keytalkvirtualappliances.blob.core.windows.net/keytalk-virtual-appliance-56...> ✓
[Browse](#)

OS type ⓘ Windows **Linux** None (data disk)

* Size ⓘ 16 GiB
Standard HDD
[Change size](#)

Note: While a Standard HDD suffices, you may want to use an SSD for improved performance

Step 5: Create a VM from the created disk

Home > **Disks** > KeyTalk_SMIME_LDAP_HA

KeyTalk_SMIME_LDAP_HA
Disk

Search (Ctrl+/) « **+ Create VM** + Create snapshot Delete

Overview
Activity log
Access control (IAM)

Resource group (change)
[KeyTalk_Virtual_Appliances](#)

Disk state
Unattached

* Subscription Pay-as-you-go

* Resource group KeyTalk_Virtual_Appliances
[Create new](#)

Instance details

* Virtual machine name My-KeyTalk-SMIME-LDAP-Server ✓

* Region (Europe) West Europe

Availability options No infrastructure redundancy required

* Image KeyTalk_SMIME_LDAP_HA
[Browse all public and private images](#)

* Size **Standard B2ms**
2 vcpus, 8 GiB memory
[Change size](#)

Review + create < Previous Next : Disks >

Step 6: Go to the Virtual Machine and note the assigned public IP and internal IP for DNS resolving

Step 7: Add inbound ports (see chapter 1)

My-KeyTalk-SMIME-LDAP-Server - Networking

Virtual machine

Search (Ctrl+/) « Attach network interface Detach network interface

Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems

Settings
Networking
Disks
Size
Security
Extensions

Network Interface: **my-keytalk-smime-lda754** Effective security rules Topology
Virtual network/subnet: KeyTalk_Virtual_Appliances-vnet/default NIC Public IP: **40.113.138.133** NIC Private IP: **10.0.0.6** Accelerated networking: Disabled

Inbound port rules Outbound port rules Application security groups Load balancing

Network security group My-KeyTalk-SMIME-LDAP-Server-nsg (attached to network interface: my-keytalk-smime-lda754)
Impacts 0 subnets, 1 network interfaces

Add inbound port

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBou...	Any	Any	AzureLoadBala...	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny