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**
	3000	**Management UI access**
TCP out:	**53**	**DNS**
	80	**KeyTalk virtual appliance**
	123	**NTP**
	443	**KeyTalk virtual appliance**
	443	**ldapupgrade.keytalk.com LDAP OS security update fetch**
	7999	**stash.keytalk.com LDAP firmware updates (SSH protocol)**
UDP out:	**514**	**Syslog/SIEM**

2 Setup

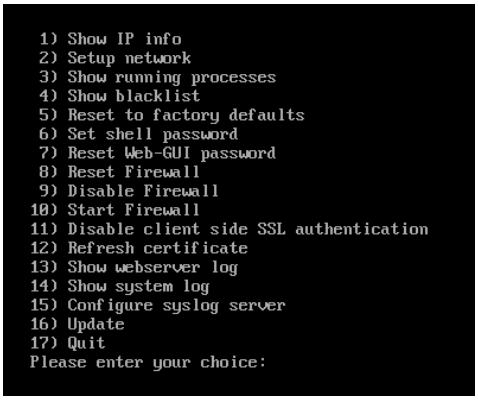
2.1 Basic network configuration

DHCP is default used to assign networking.

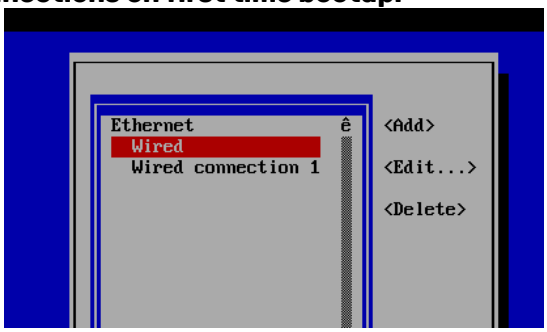
To manually set your IP for the first time perform the following:

1) **From your CLI login:**
   Username: keytalk
   Password: Change!

2) **After successful authentication the following options are provided:**

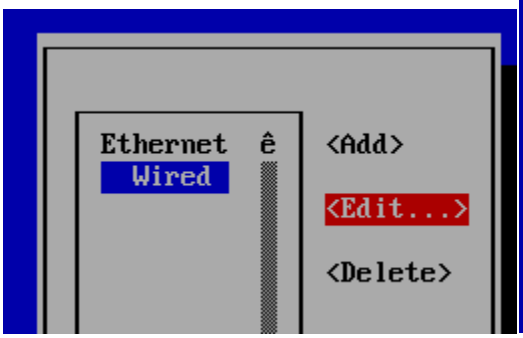


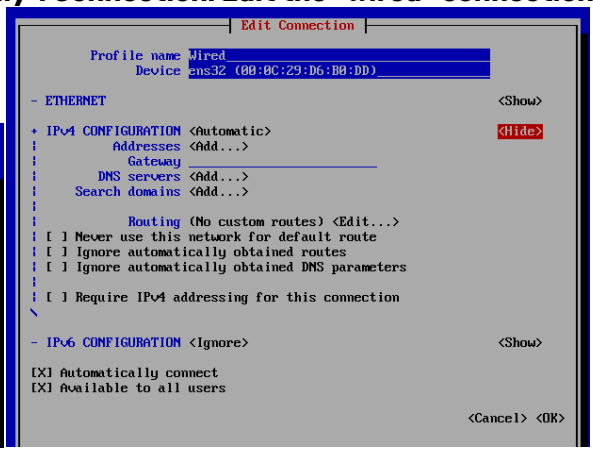
3) **Select 2) to setup your network, and** remove any shown connections**, as Hypervisors tend to add unwanted additional connections on first time bootup.**



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

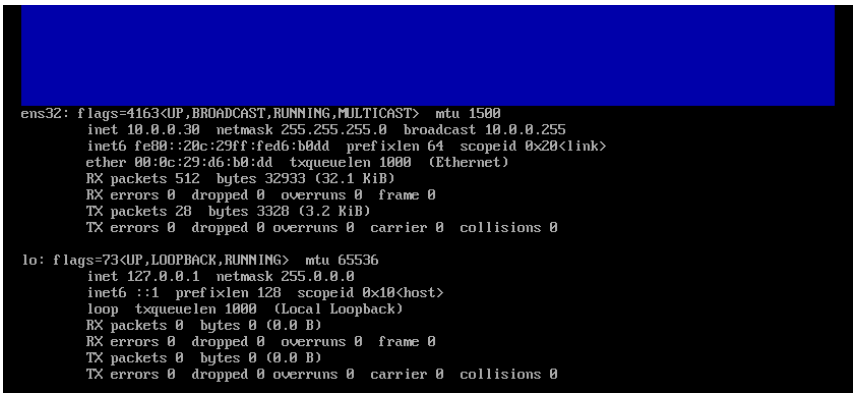
4) **The virtual appliance will now show only 1 Connection. Edit the "Wired" connection:**





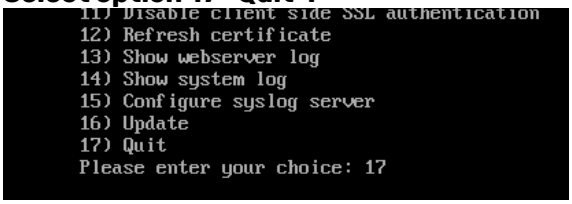
Ensure you select: Manual and add the relevant networking
To set your subnetmask add the appropriate / (slash forward)to your IP, ref:
https://www.aelius.com/njh/subnet_sheet.html
NTP is fetched from the Hypervisor or from https://time.is/UTC
! DO NOT SET THE FQDN OR HOST NAME YET !

5) **Select OK to apply the changes:**

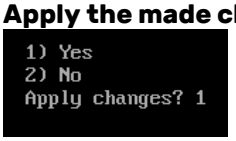


Press any key to return to the initial configuration menu

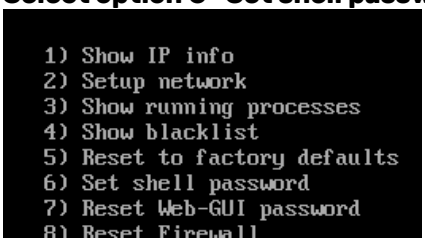
6) **Select option 17 "Quit":**



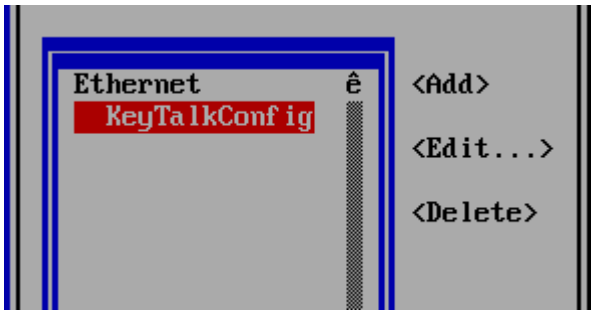
Apply the made changes:



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



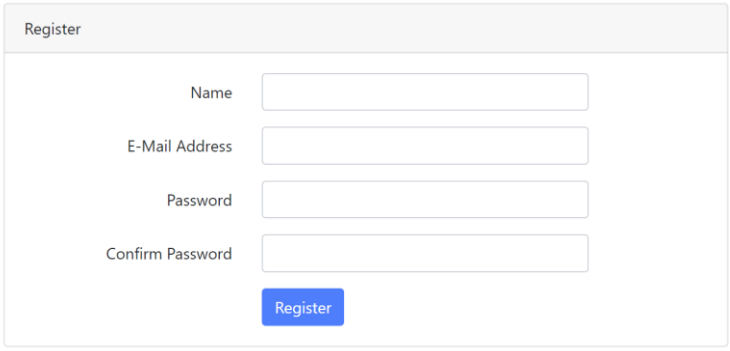
NOTE: **When the management web UI (port 3000/login) is used to at least once make changes to the network, the default "Wired" connection will be renamed to KeyTalkConfig**



2.2 KeyTalk LDAP management UI setup : activation and SSL

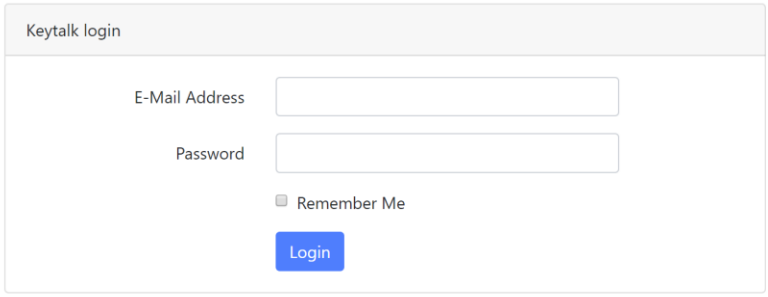
In order to configure the actual LDAP functionality, perform the following steps:

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

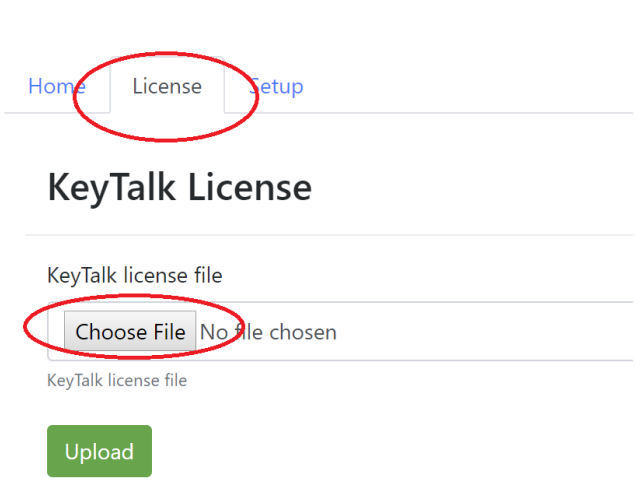


Note: **An SSL trust error will happen as the virtual appliance comes with a self signed expired SSL certificate**

Step 2:Access the admin GUI on:
https://<ipaddress>:3000/login
Username: <yourchosenadminusername>
Password: <yourchosenpassword>



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

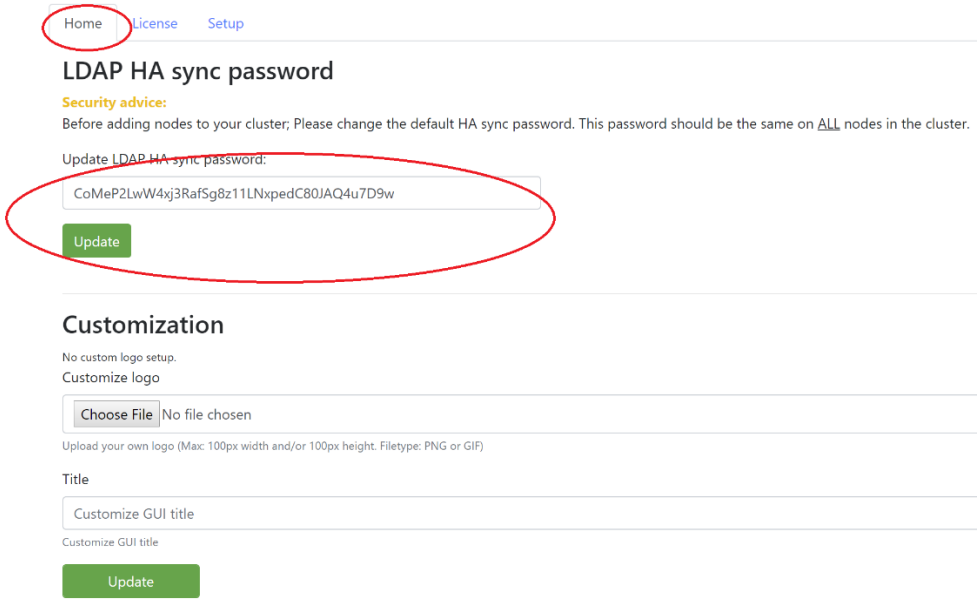


Step 4: Change the LDAP HA sync password

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.

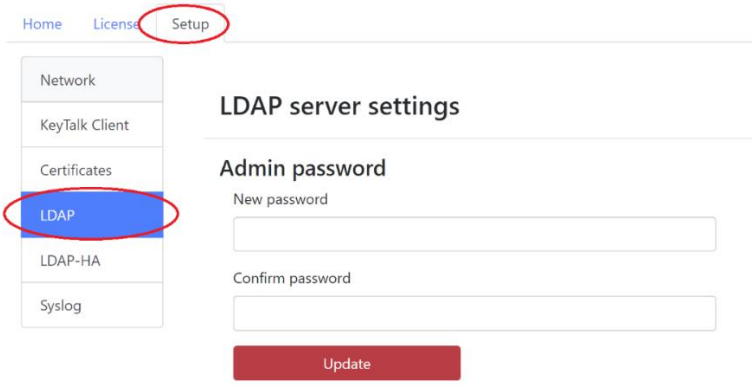
To change it, the KeyTalk LDAP will generate a random which renews when you refresh the page. When you see a random you like, select UPDATE
Write down / cope on a secure location this password for future references, as you will need to enter the same sync password on all your KeyTalk LDAP nodes when 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.



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)



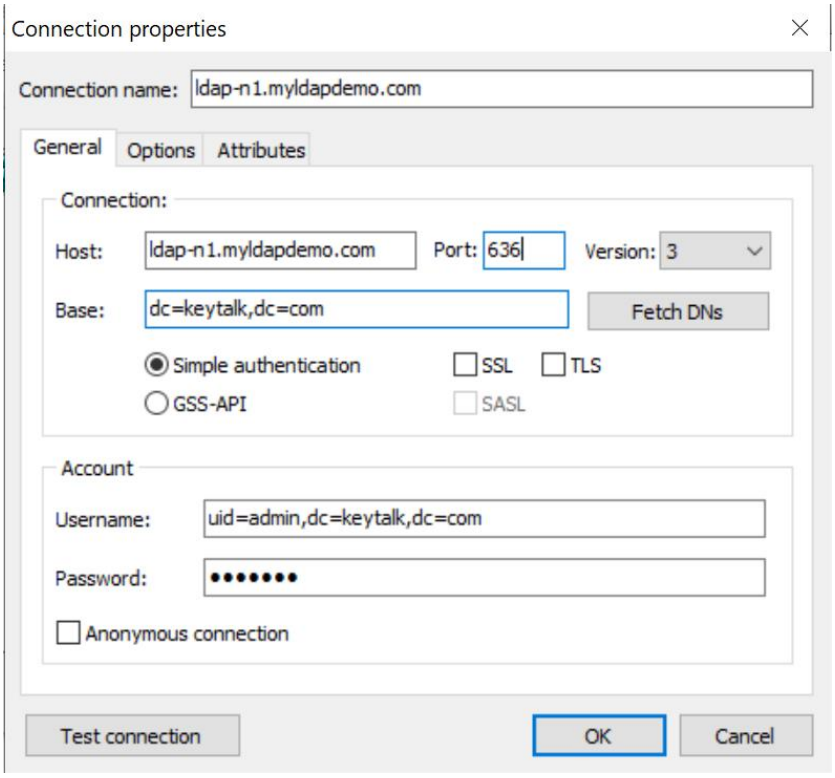
The LDAP Base DN is: **dc=keytalk,dc=com**
The LDAP Bind DN is: **uid=admin,dc=keytalk,dc=com**
The LDAP username is: **admin**
OU: **People**

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

Configure LDAP Server connection for Service ldaptest

URL: *	ldap://ldap-n1.myldapdemo.com:389 or ldaps://ldap-n1.myldapdemo.com:636
Bind DN: *	uid=admin,dc=keytalk,dc=com
Bind Password: *	••••••• show
Allow empty password:	
Base DN: *	ou=people,dc=keytalk,dc=com
Service User:	admin
Service Password:	••••••• show
Is Active Directory:	
Address Book only:	
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**



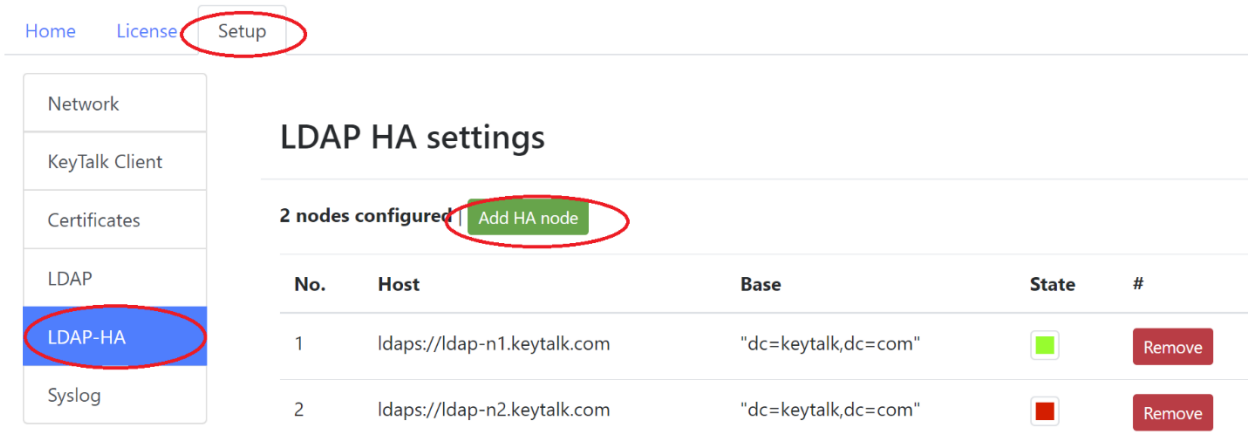
Step 6: Set the LDAP (node) FQDN hostname

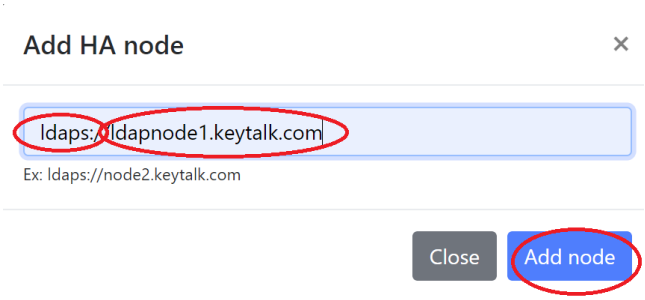
For production purposes, it is important to follow this step.

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.

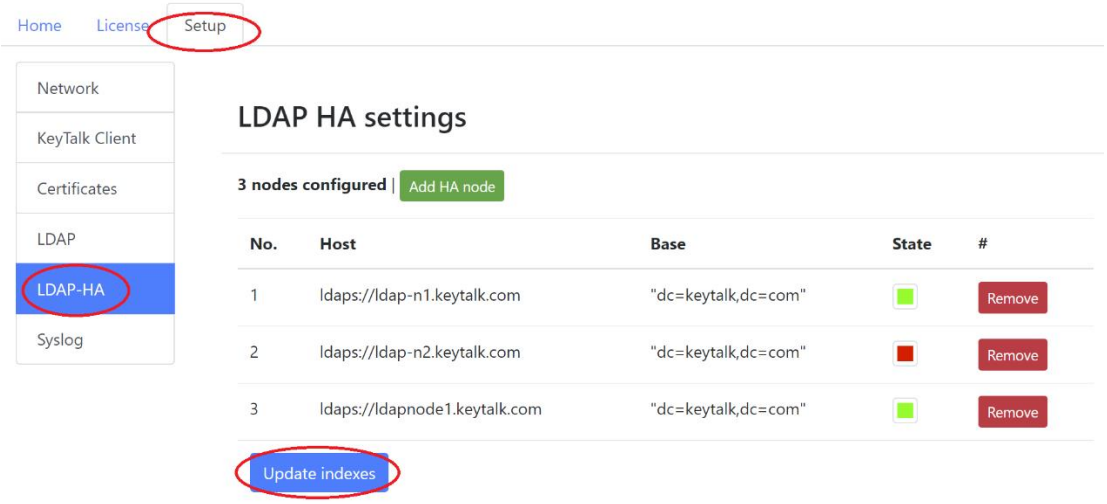
Contrary to what would be expected, due to High Availability functionality, changing the hostname, first requires a new DNS resolvable LDAP HA-node to be added. So ensure a DNS entry matching the FQDN exists and points to the IP of the LDAP instance you're configuring

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)

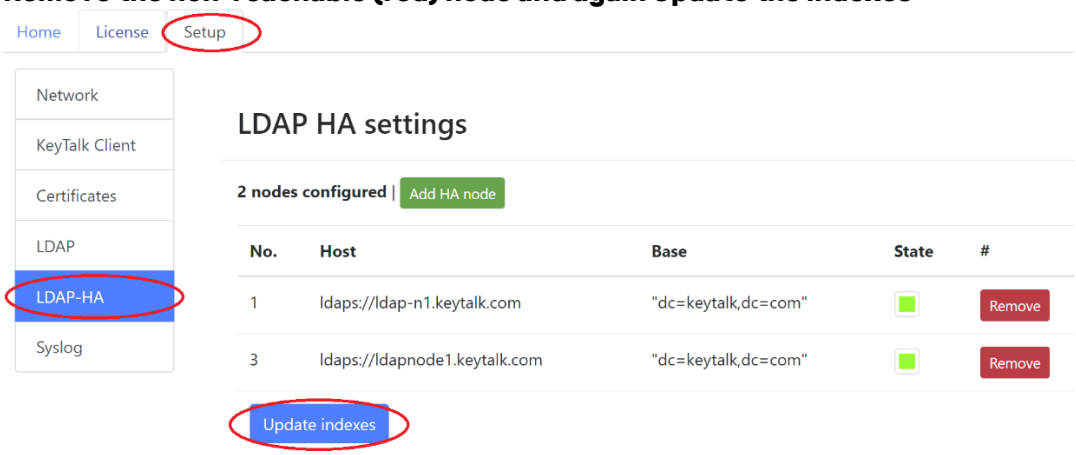




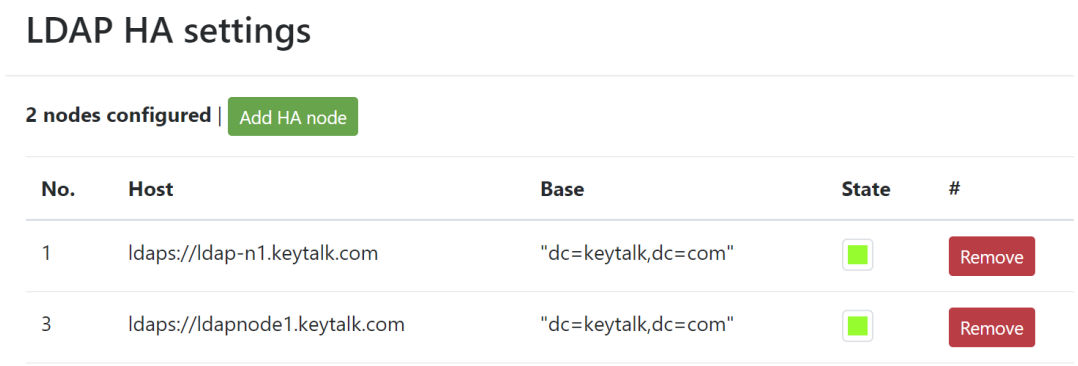
Now update the indexes:



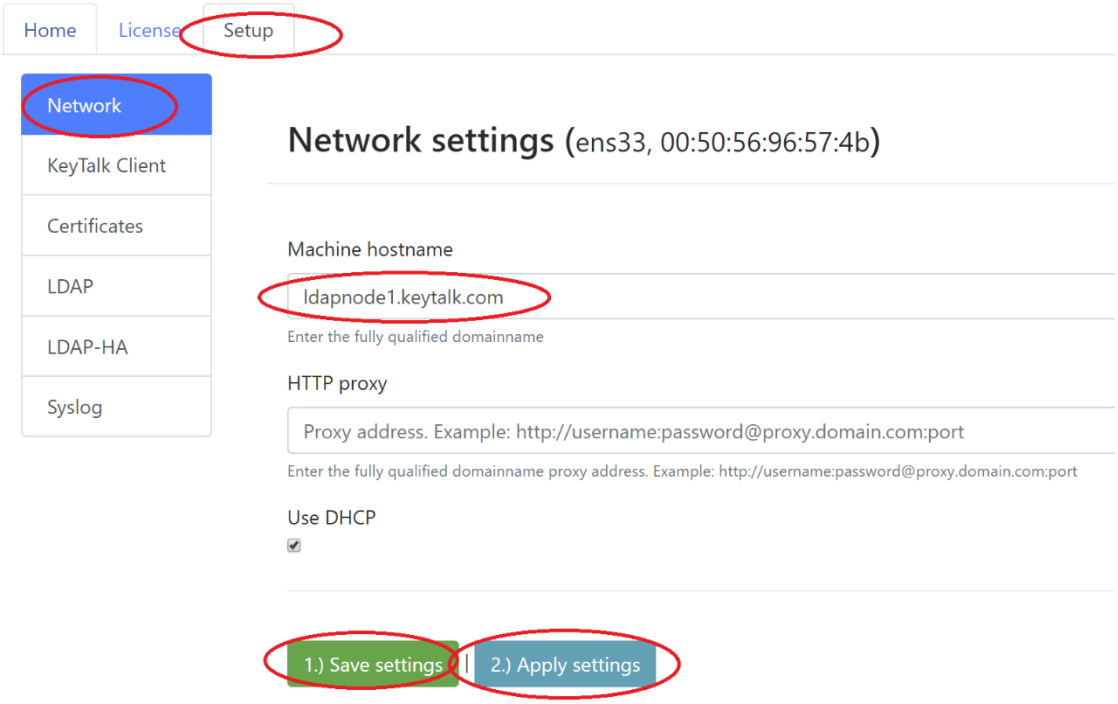
Remove the non-reachable (red) node and again Update the indexes



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



Now change your hostname:



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

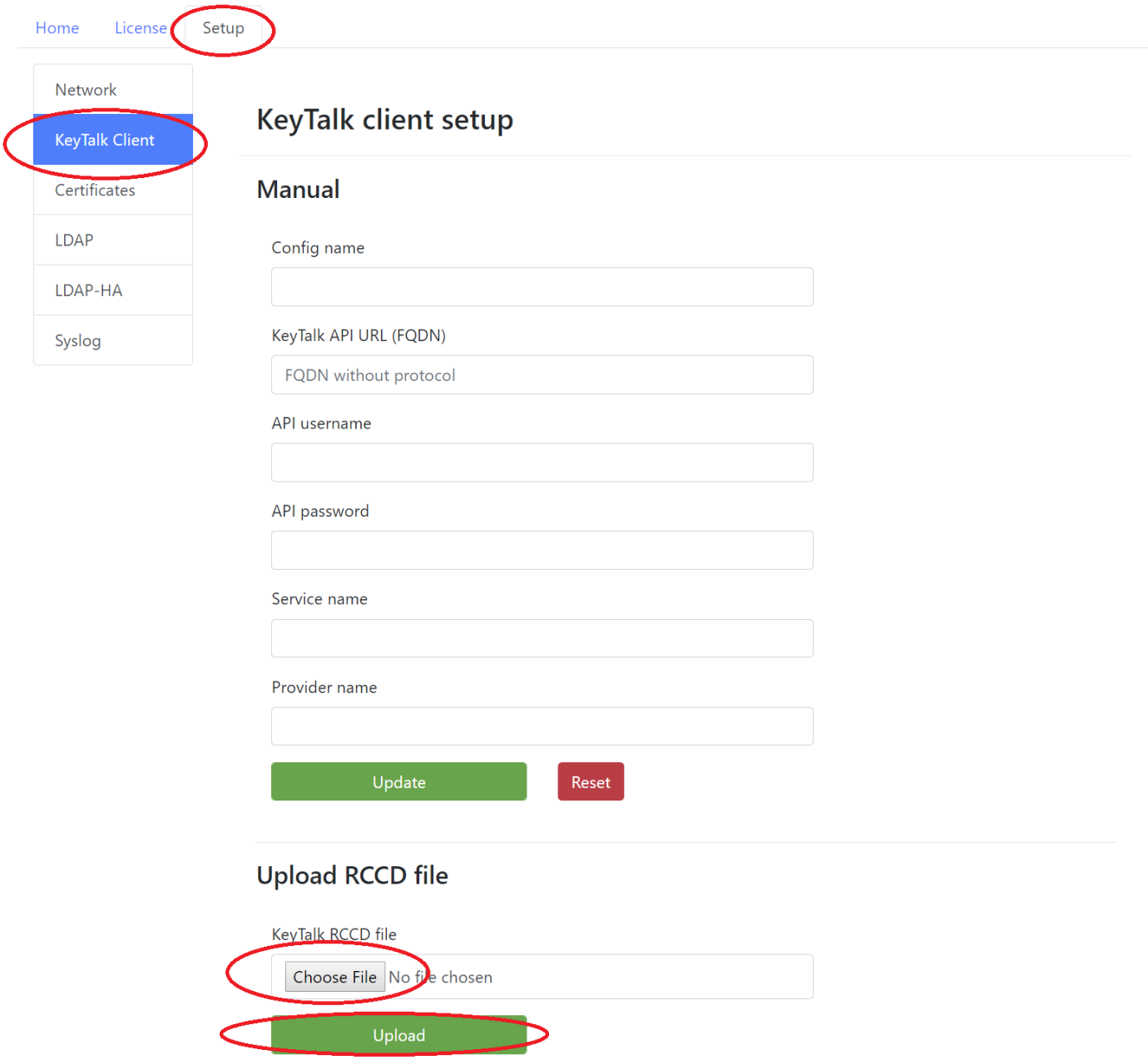
Step 7: Install an SSL certificate

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

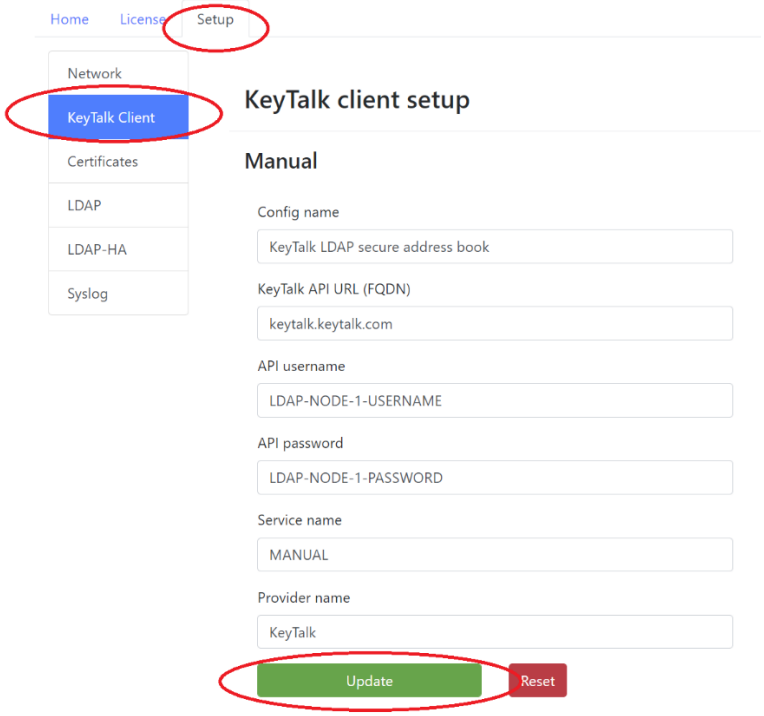
The KeyTalk LDAP secure email address book supports certificate lookup based on HTTPS and LDAP / LDAPS
Adding an SSL certificate ensures LDAPS and HTTPS can be used, whereby LDAPS is also used for HA synching between LDAP nodes provided it is indicated in the discoverable HA node list.

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*

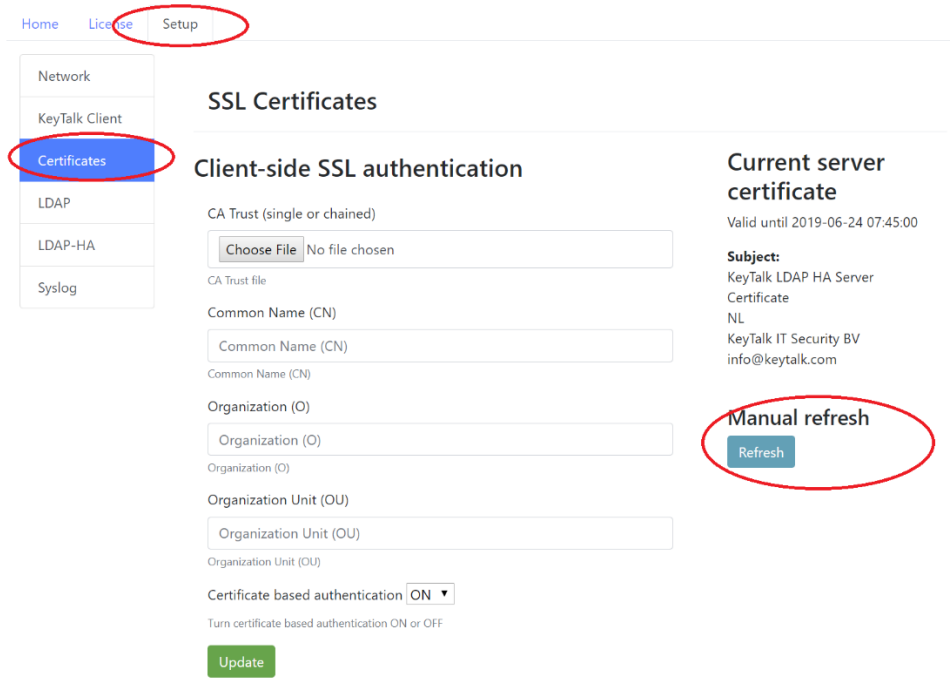
First upload the appropriate KeyTalk RCCD file, that links to the proper KeyTalk SERVICE under which the SSL certificate is obtained and managed.



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



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



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:**

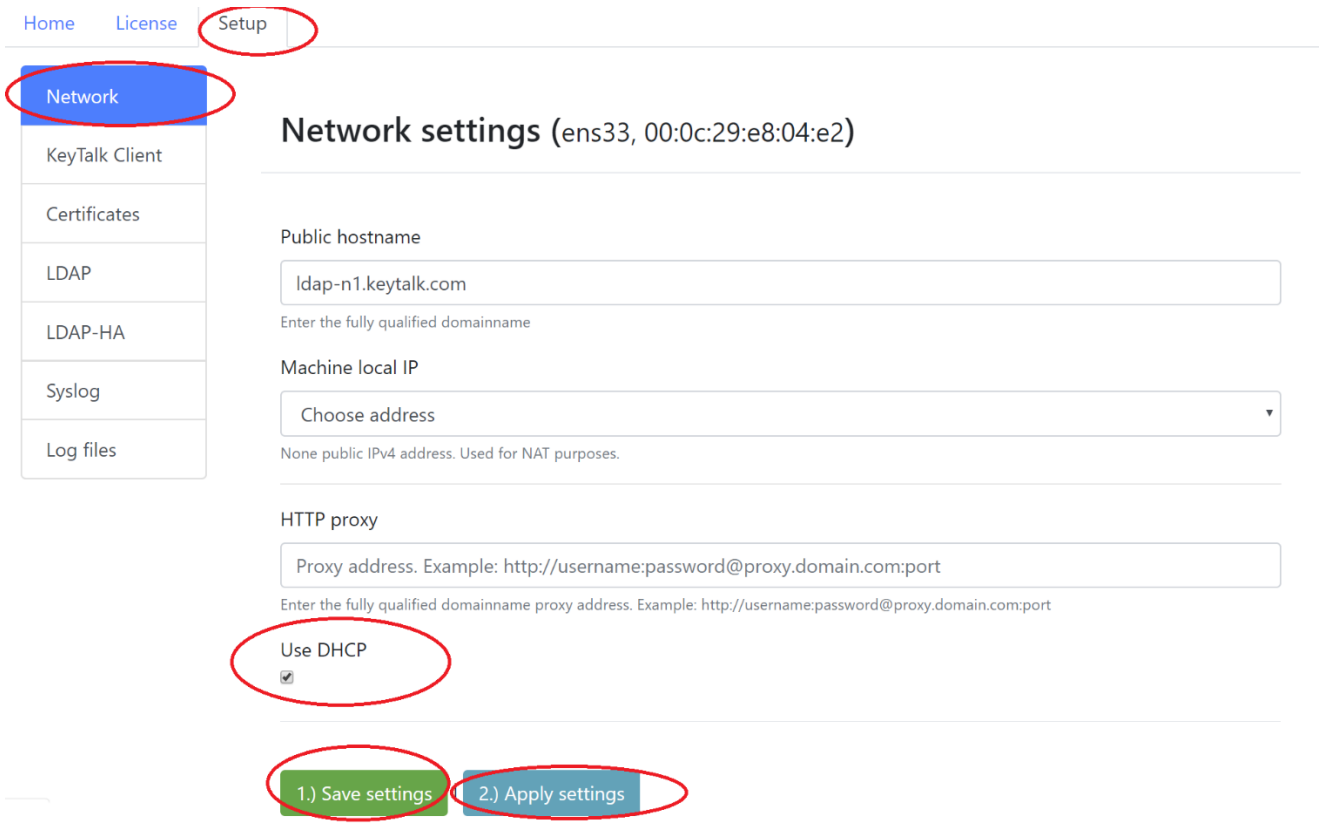
I) The certificate was found to be revoked due to CRL
II) The certificate has expired
III) The certificate is about to expire based on the threshold time set in the KeyTalk RCCD parameters

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.

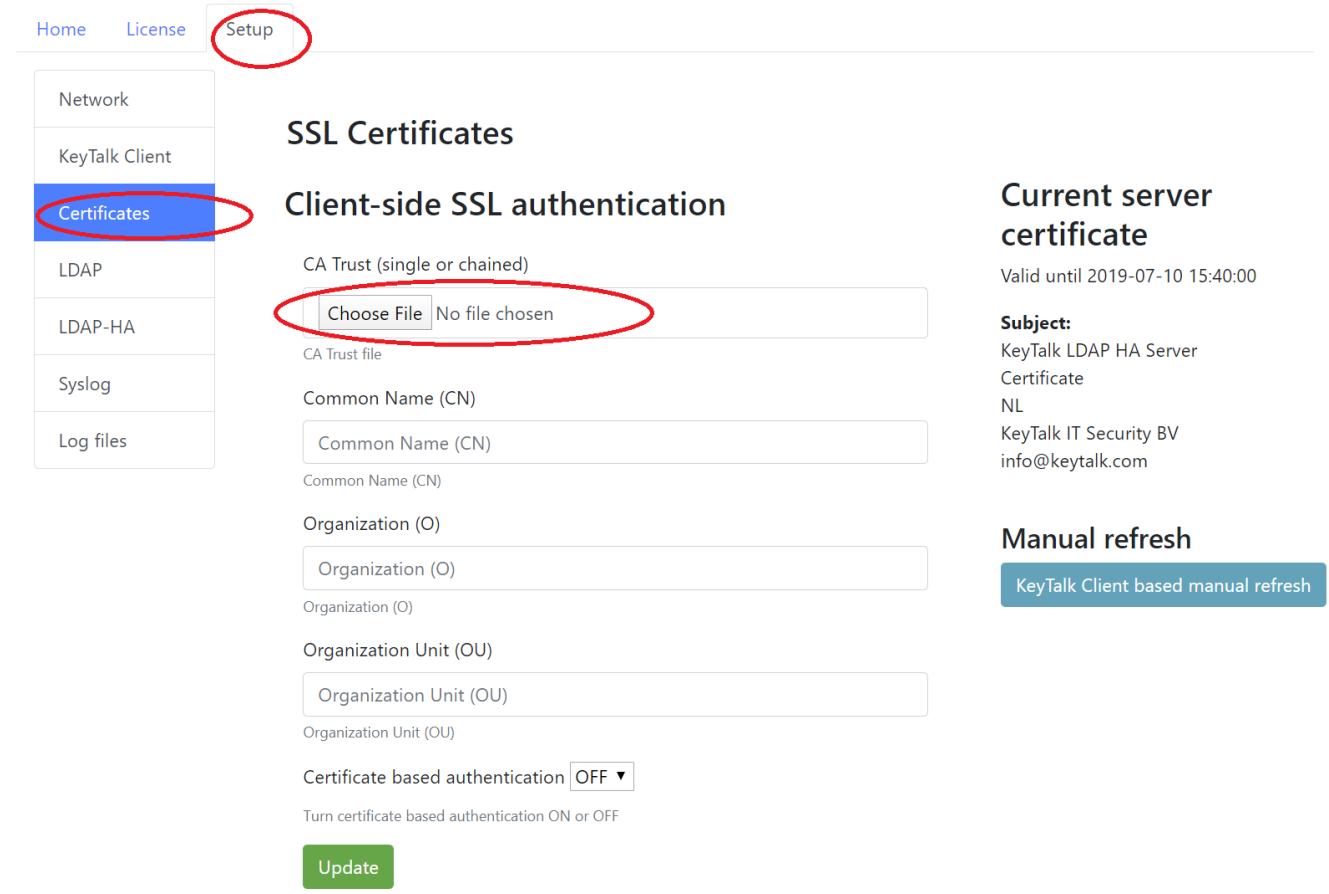
When making changes, to make these persistent:

1) save the settings
2) apply the settings.



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



Should you accidently 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

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**

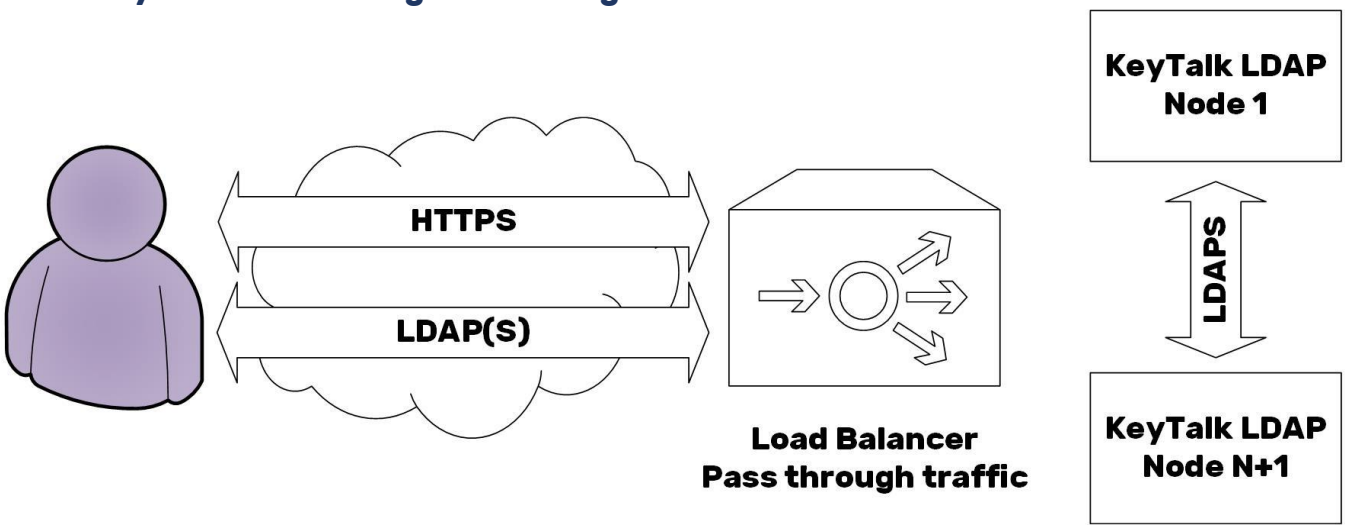
As a result for each LDAP node, you have to individually configure:

- **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).**

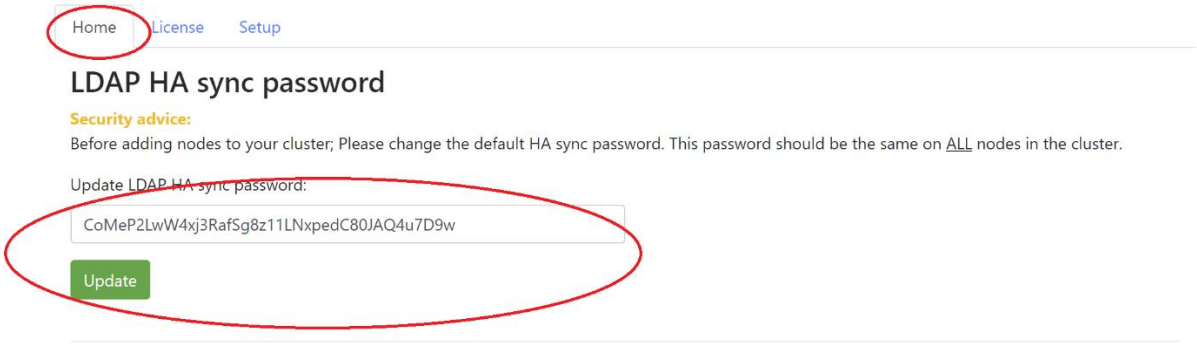
2.5.1 KeyTalk LDAP HA high over design



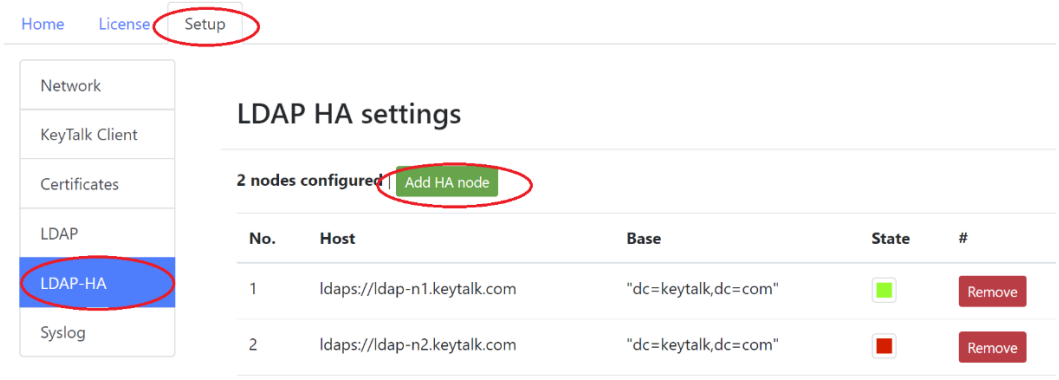
2.5.2 KeyTalk HA configuration

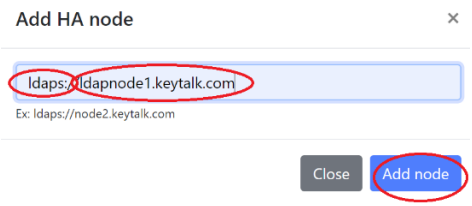
Thoroughly read all required steps first, as you may have performed some already as per the quick guide steps

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!

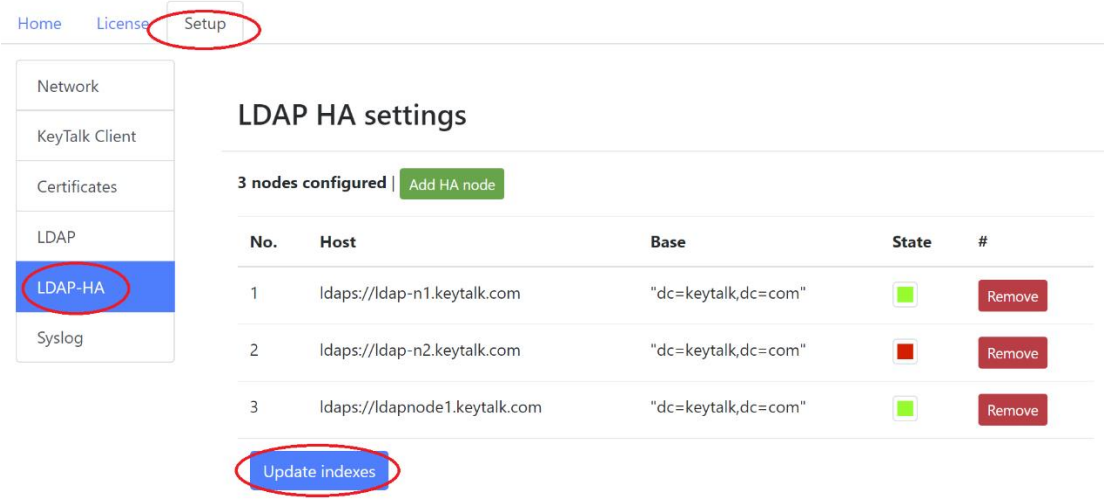


Step 2: Add the FQDN as a new HA node which represents this machine. Ensure that either ldap:// or ldaps:// is used, ie the trusted SSL certificate must be installed or ldaps won't work.

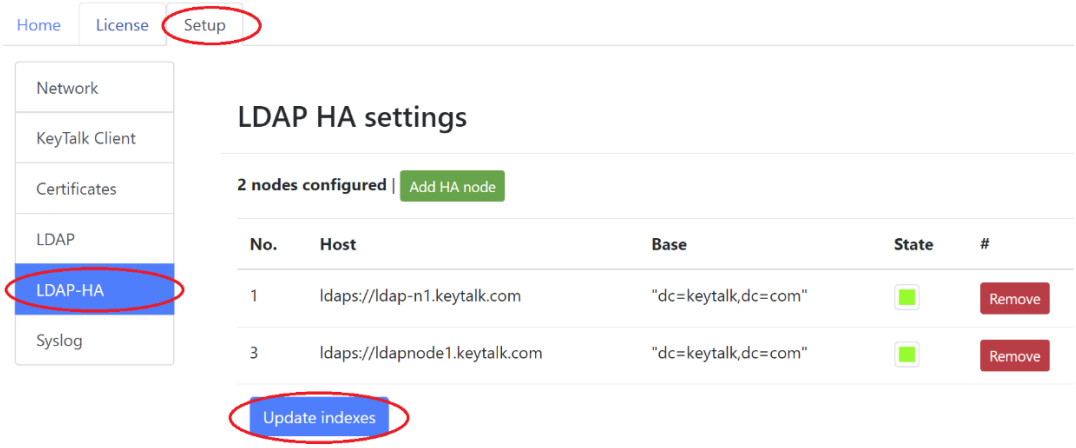




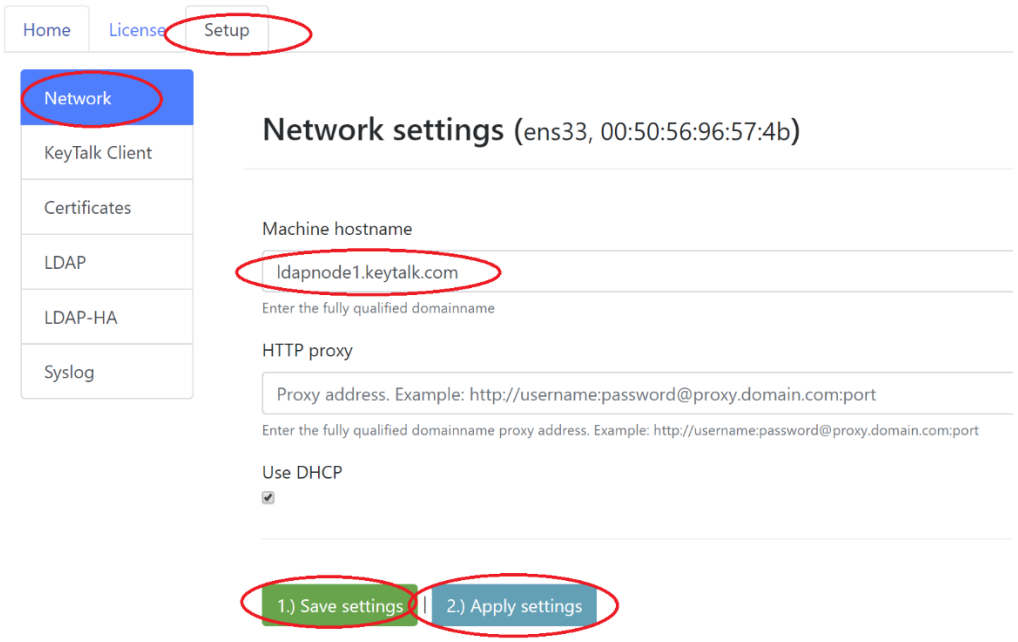
Step 3: Update the indexes:



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

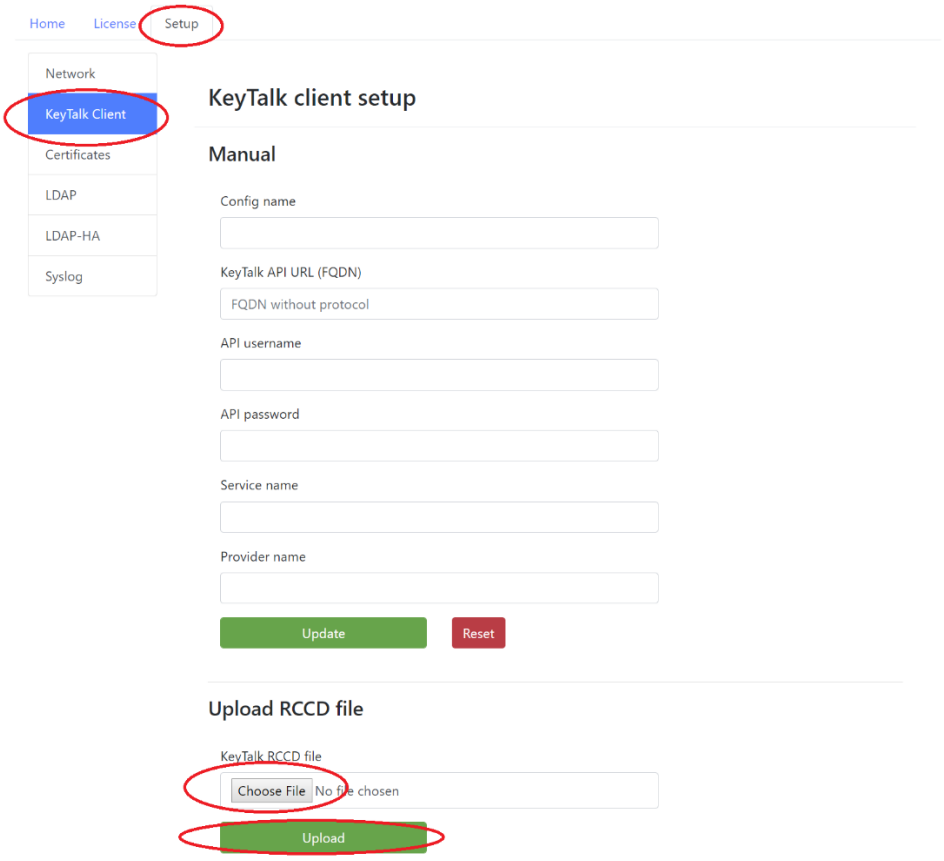


Step 5:Change your hostname:

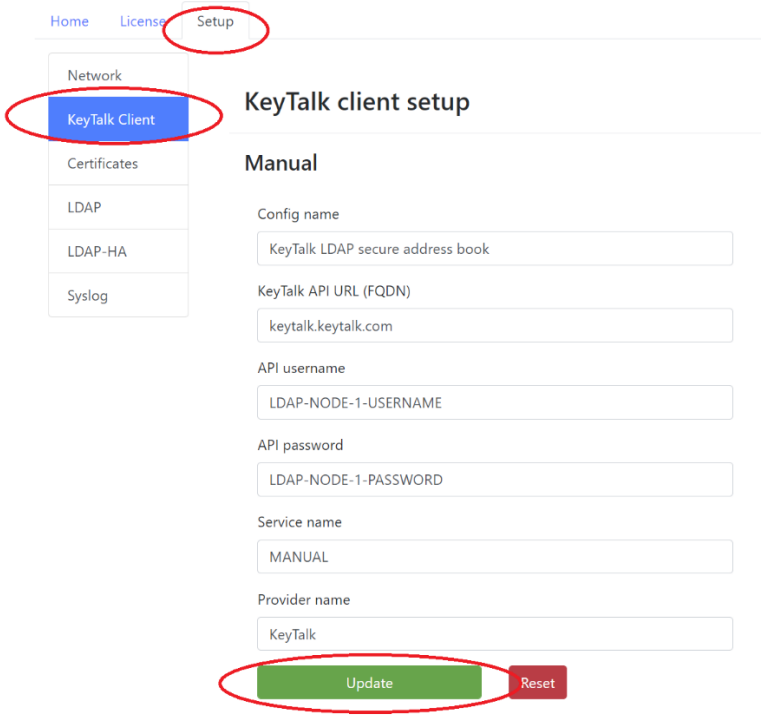


Step 6:Set the KeyTalk client details enabling the fetching of the SSL certificate to support LDAPS

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

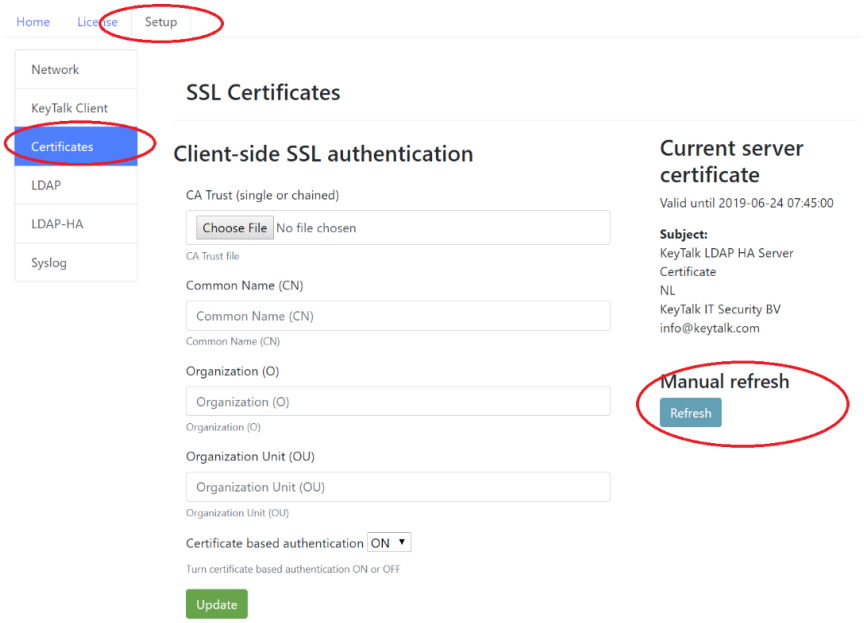


After uploading the appropriate RCCD you need to minimally configure the required authentication data:



Step 7: Install the SSL certificate

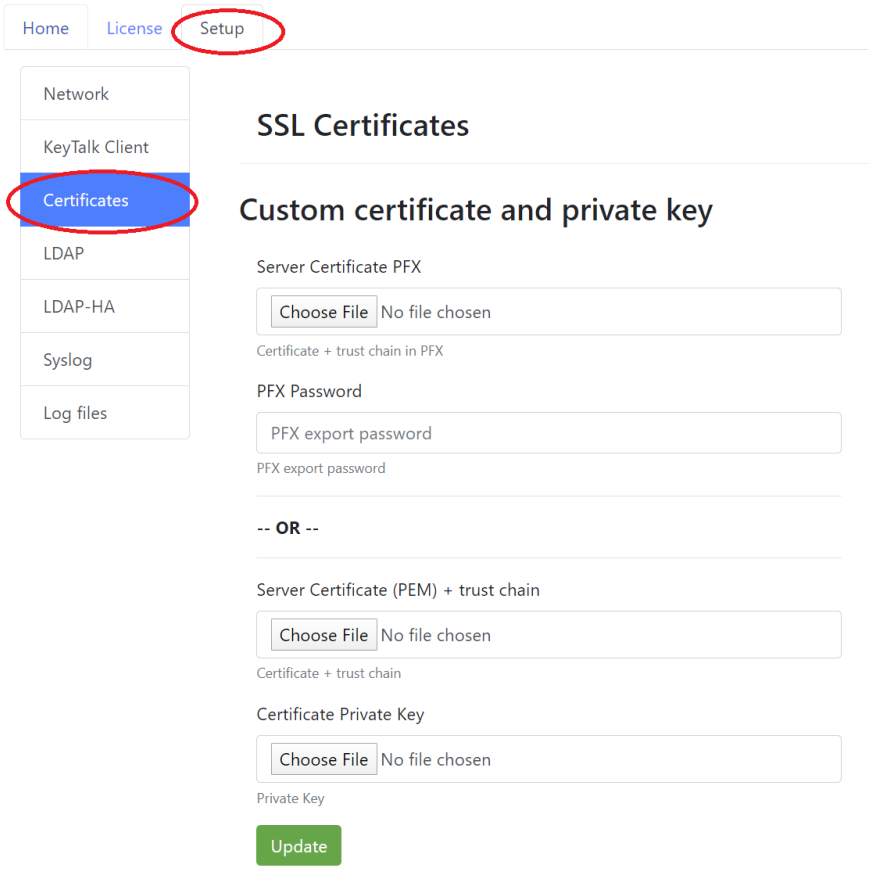
Either wait 5 minutes for the LDAP to automatically update the certificate, or manually enforce a renewal by pressing REFRESH when using the KeyTalk CLM to issue the LDAP server certificate:



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.

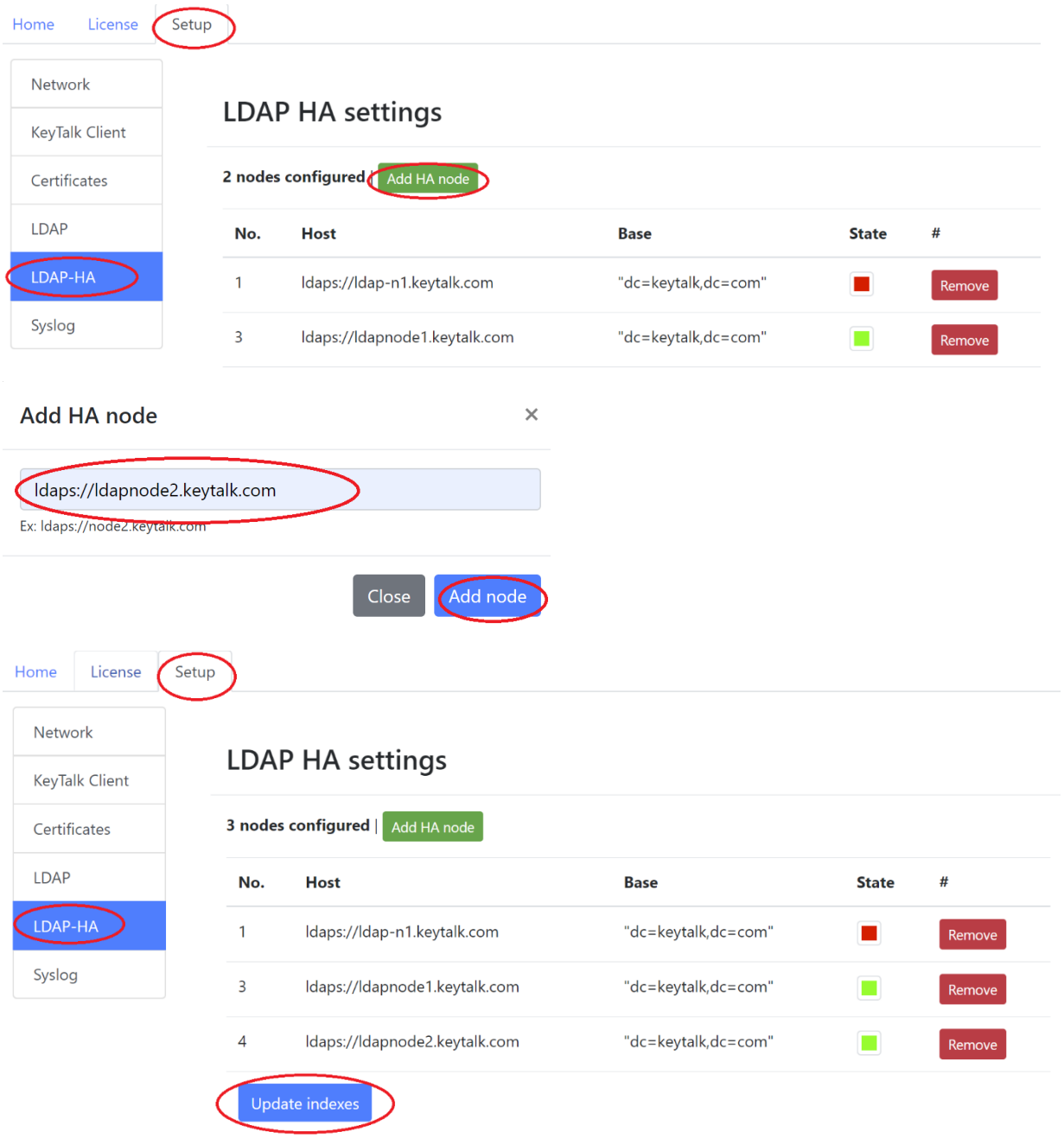
Alternatively manually upload your LDAP certificate and key:



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

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



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

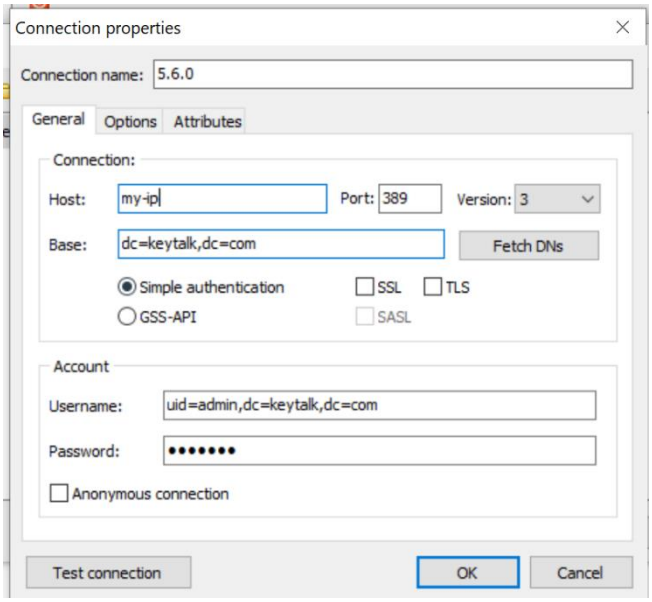
3.1 Directly accessing the LDAP for management

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**

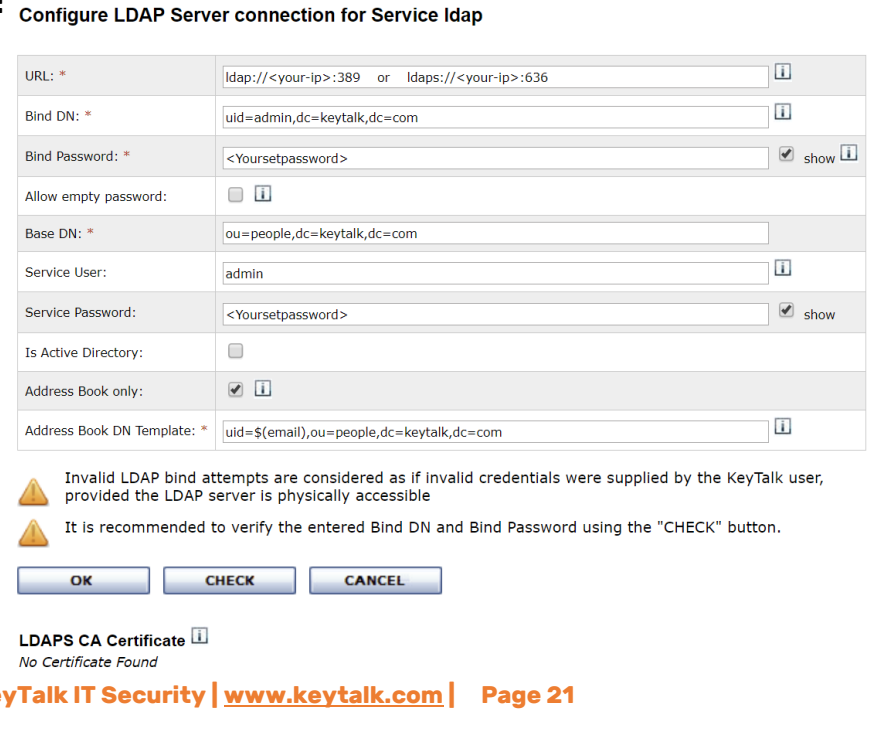


3.2 Writing KeyTalk managed certificates to the LDAP

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!) :



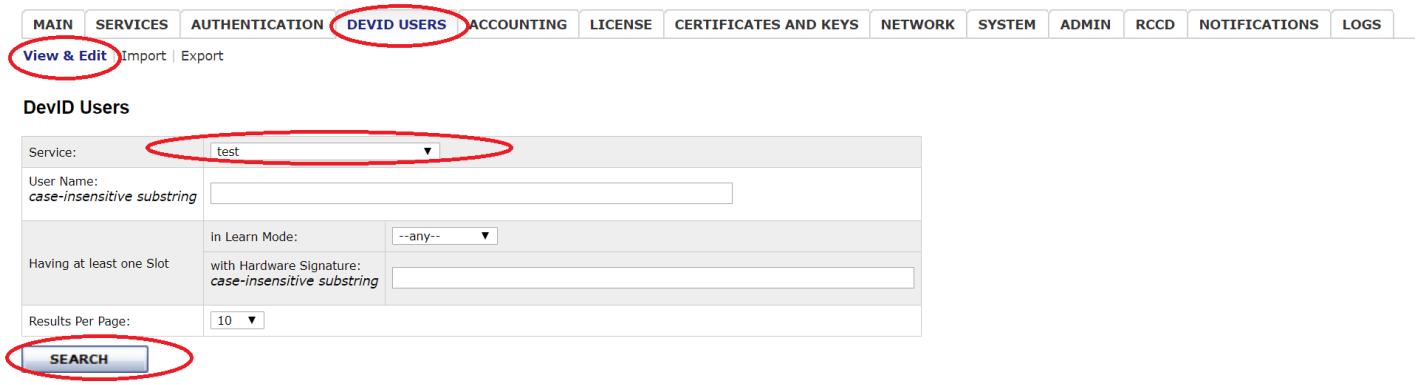
3.3 Writing non-KeyTalk managed certificates to the LDAP

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

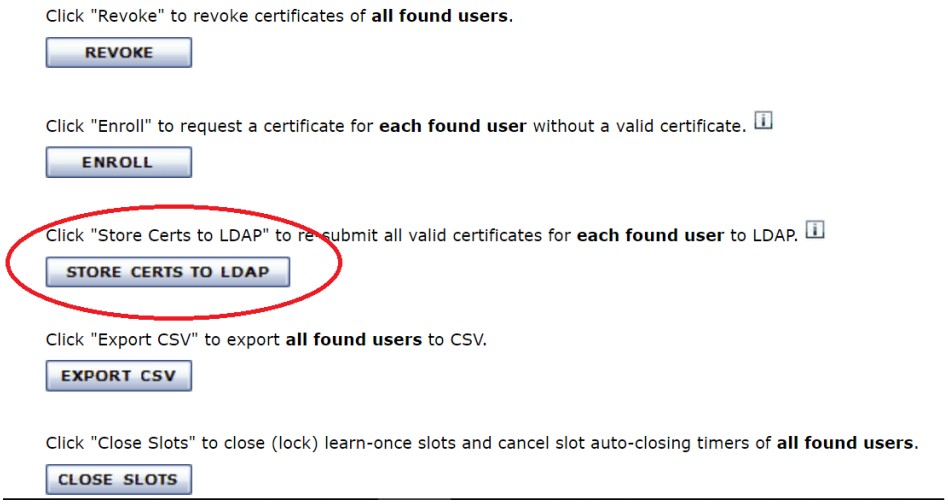
3.4 Restoring KeyTalk managed certificates to the LDAP

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 :



Now select:



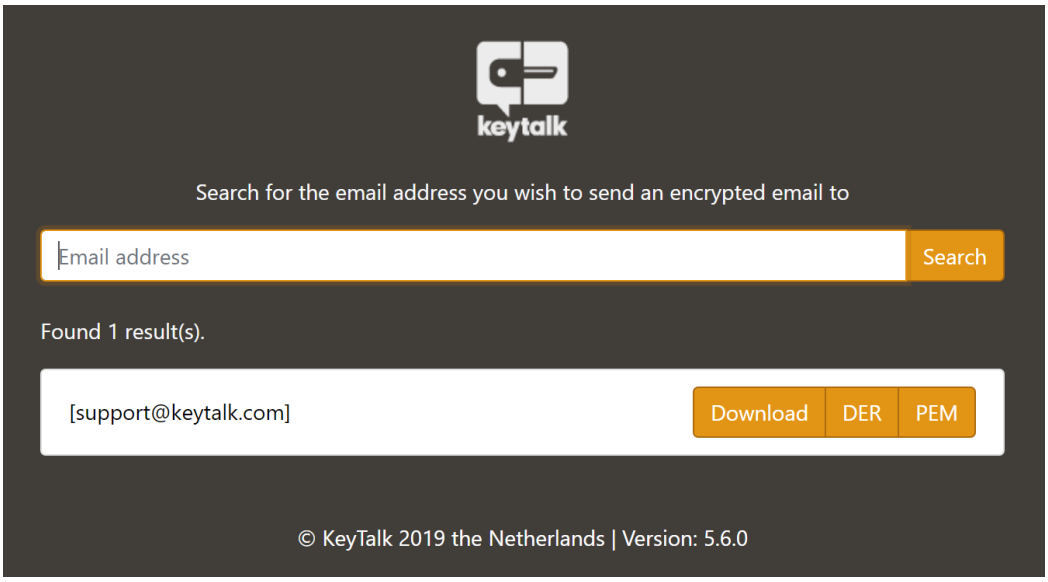
4 KeyTalk S/MIME LDAP as a web and mail client address book

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. Wilcards are not permitted.

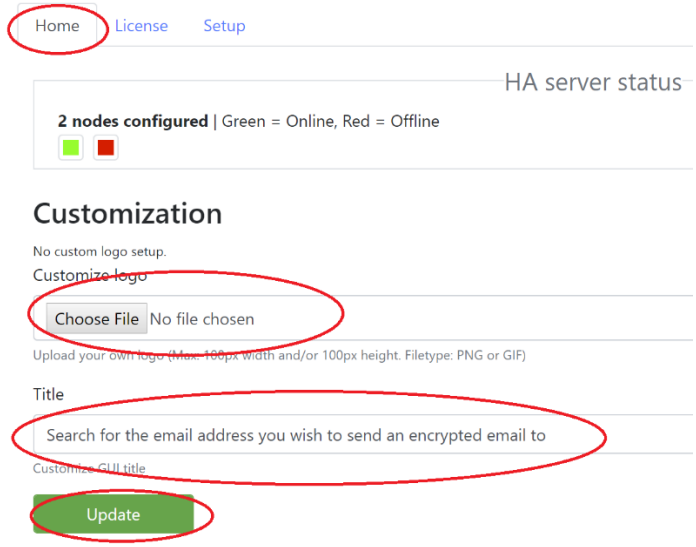


4.1 Webbased lookup basic look and feel change

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 charactersets, and can have a maximum length of 250 characters. URL links are shown as plain text only to prevent potential abuse.



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.

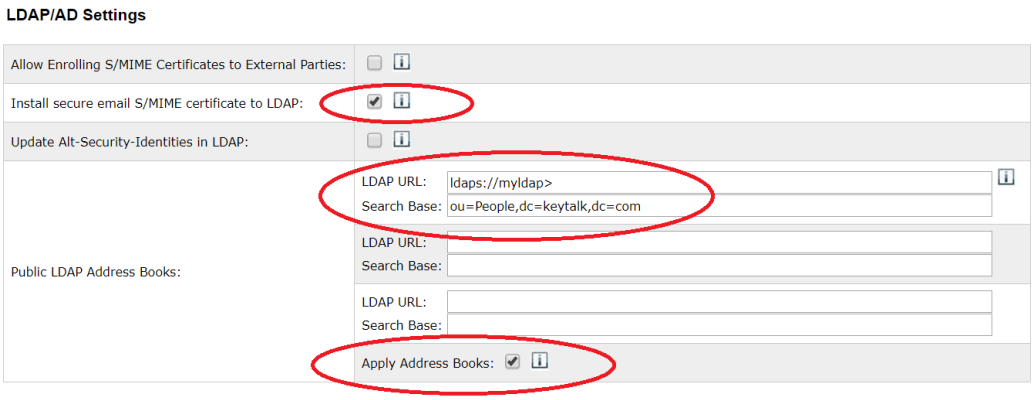
The LDAP(S) based S/MIME address search allows for a single return of a matching email address value only

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 :

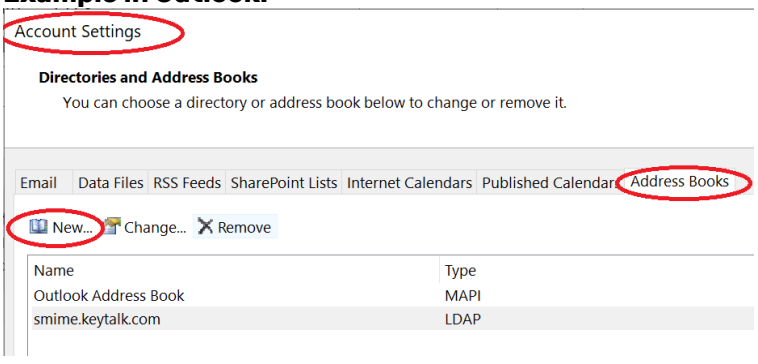


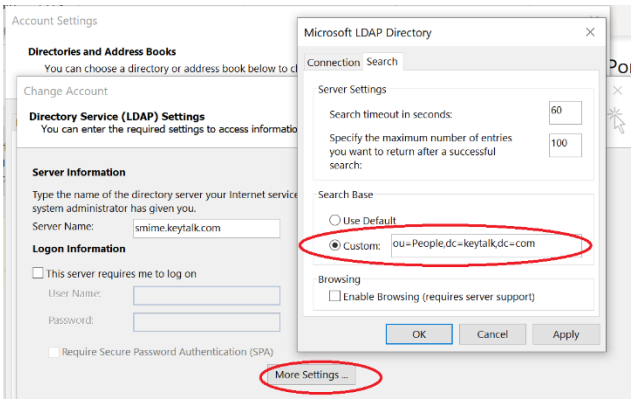
Now as soon as someone authenticates positively using the KeyTalk client, the address book is configured for either Outlook or MacMail or both when applicable.

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:





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
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
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

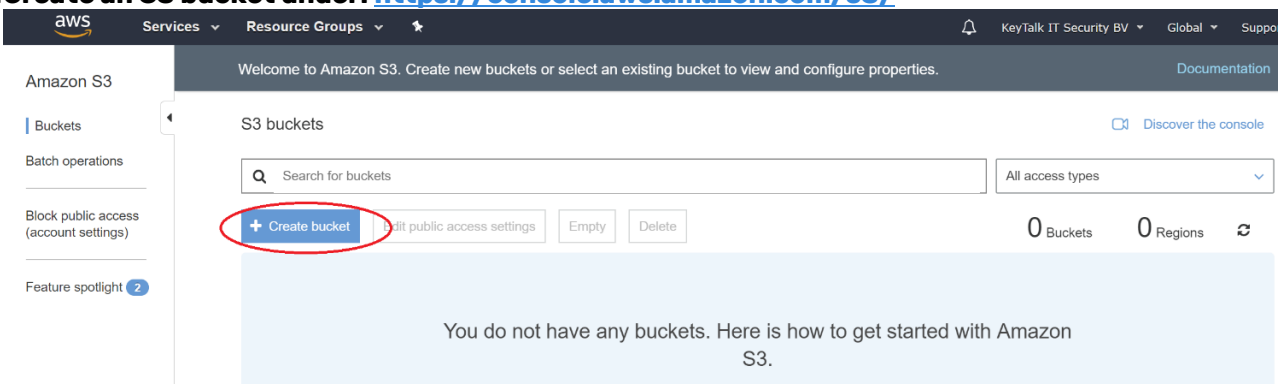
AWS online guides include:
https://aws.amazon.com/ec2/vm-import/
https://docs.aws.amazon.com/vm-import/latest/userguide/vm-import-ug.pdf
The below guide is a summary of the links above enhanced with hands-on experience.

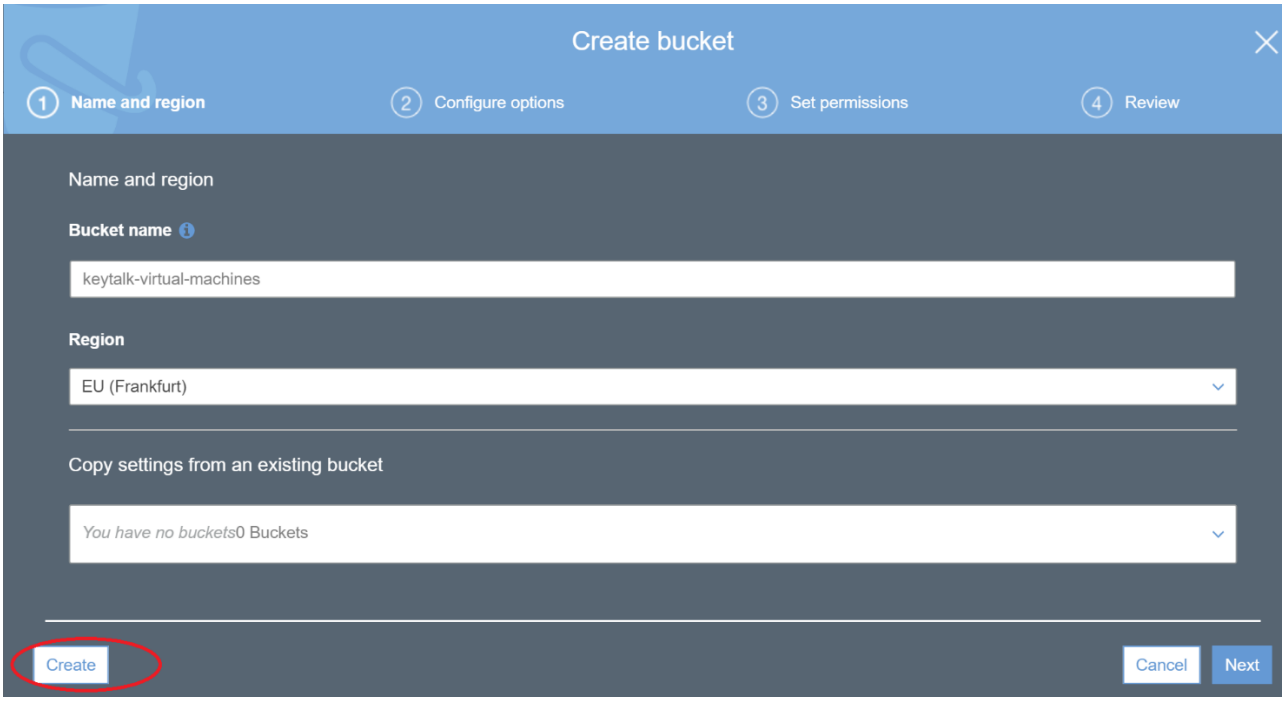
This guide assumes that you have already created an account for AWS and configured payment for it.

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/

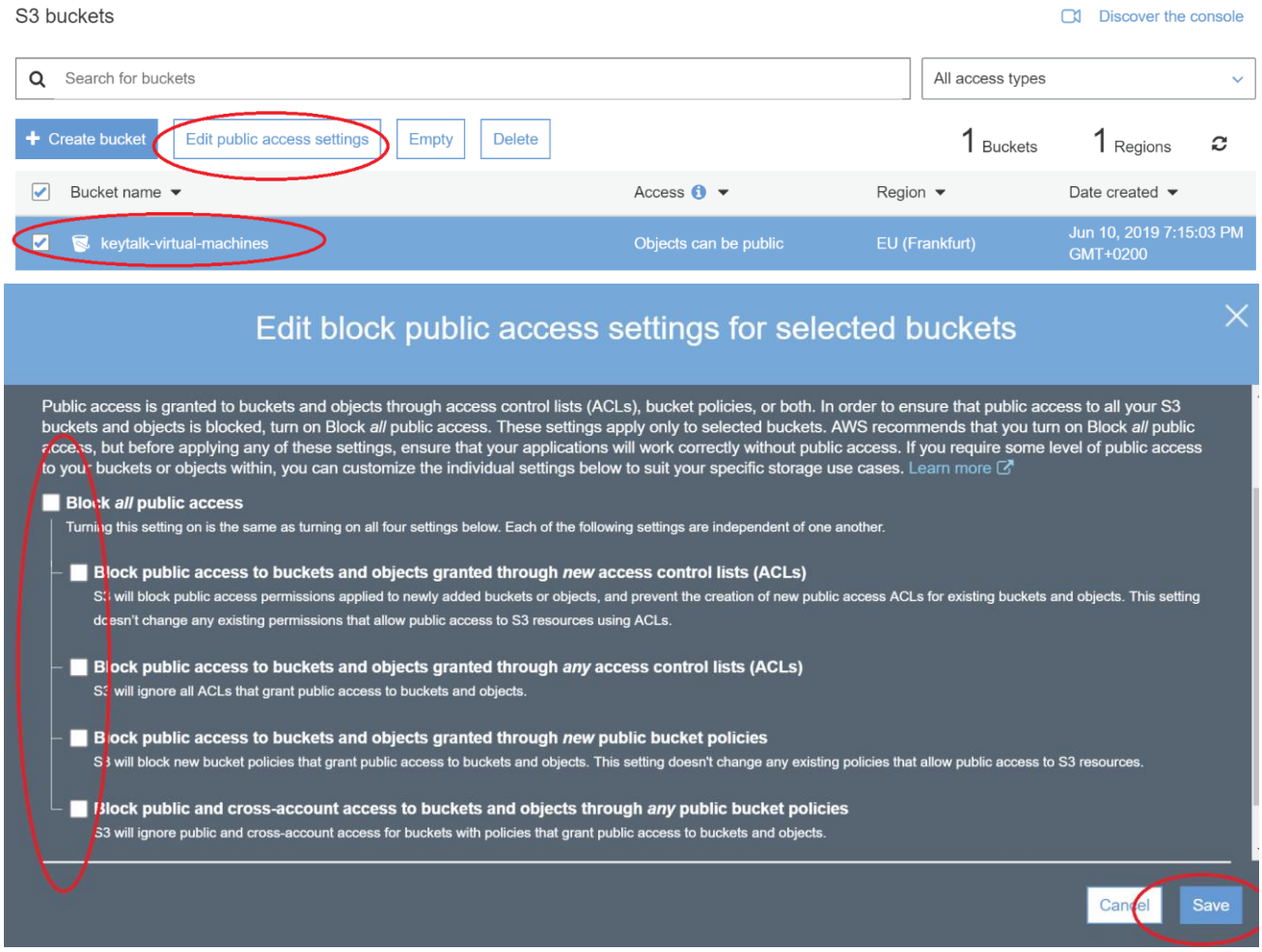
Step 3: Create an S3 bucket under: https://console.aws.amazon.com/s3/



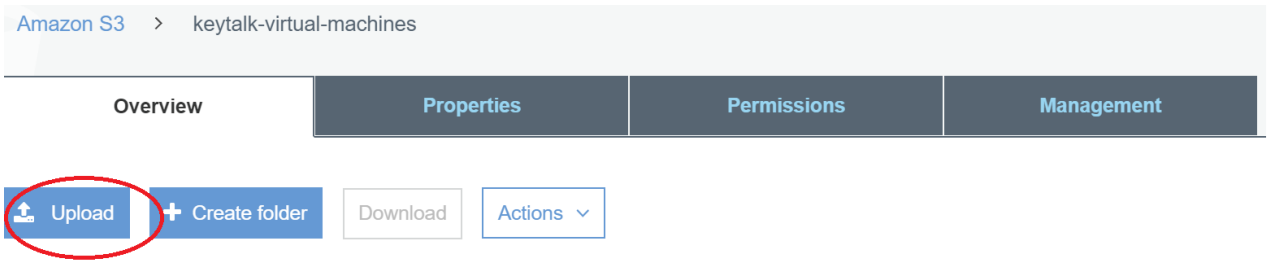


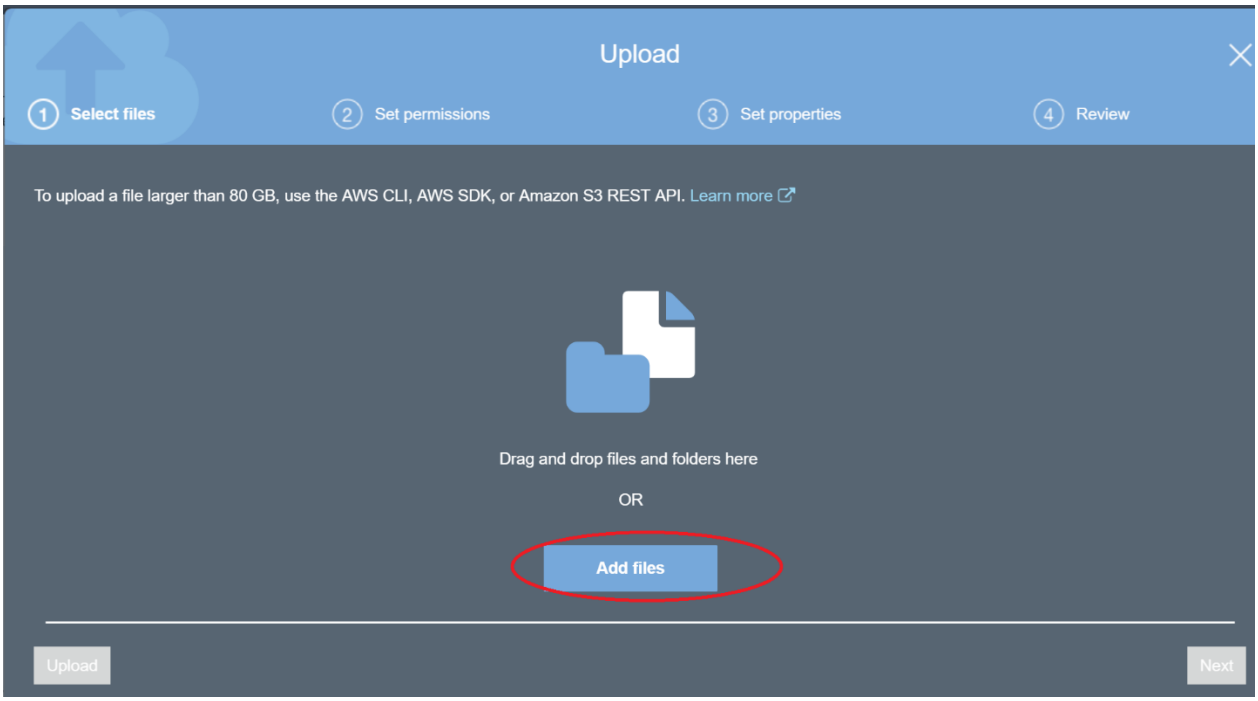
Step 4: Enable public access to the KeyTalk S3 bucket.

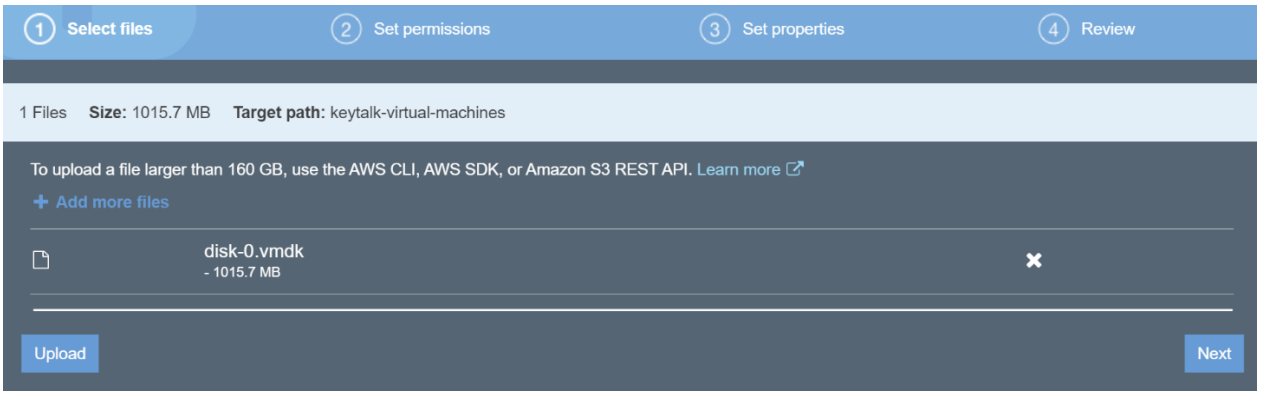
Since KeyTalk virtual appliances are public anyhow, this does not affect your security. However if this is an issue, feel free to close public access to the S3 bucket after importing the virtual machine into EC2 at the end of this guide.

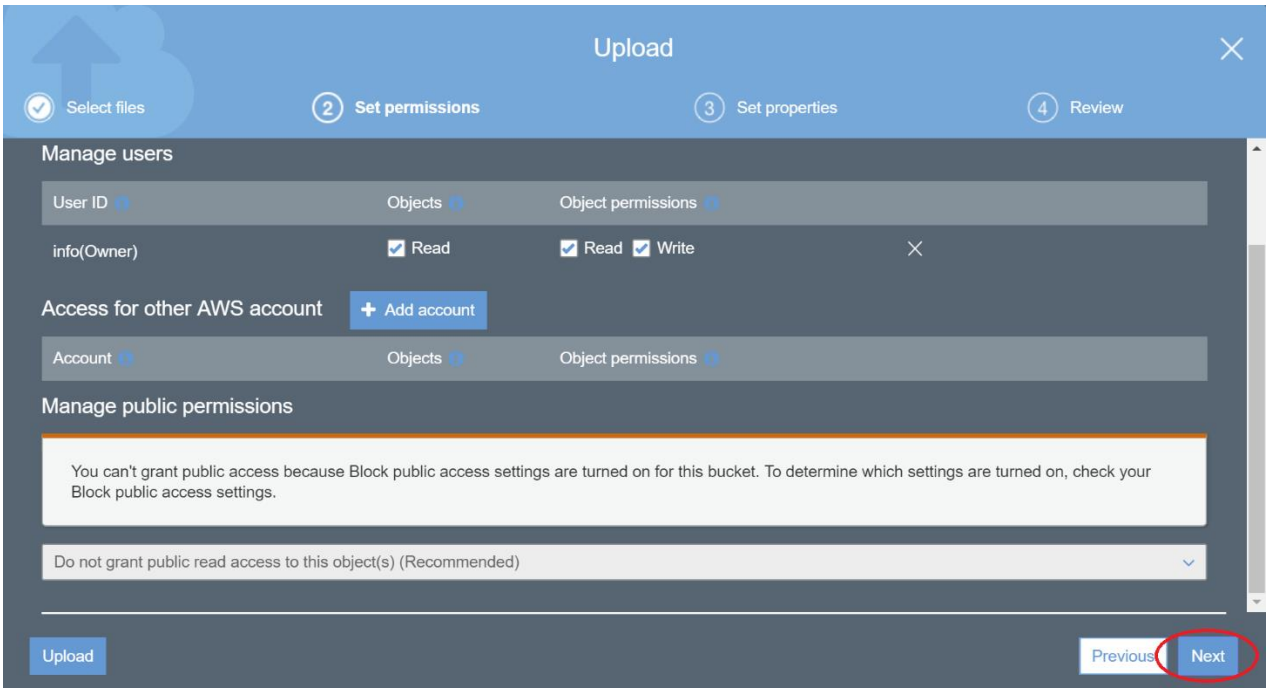


Step 5: Select the created bucket and upload your KeyTalk LDAP secure email address book virtual appliance whereby you minimally upload the included VMDK file:

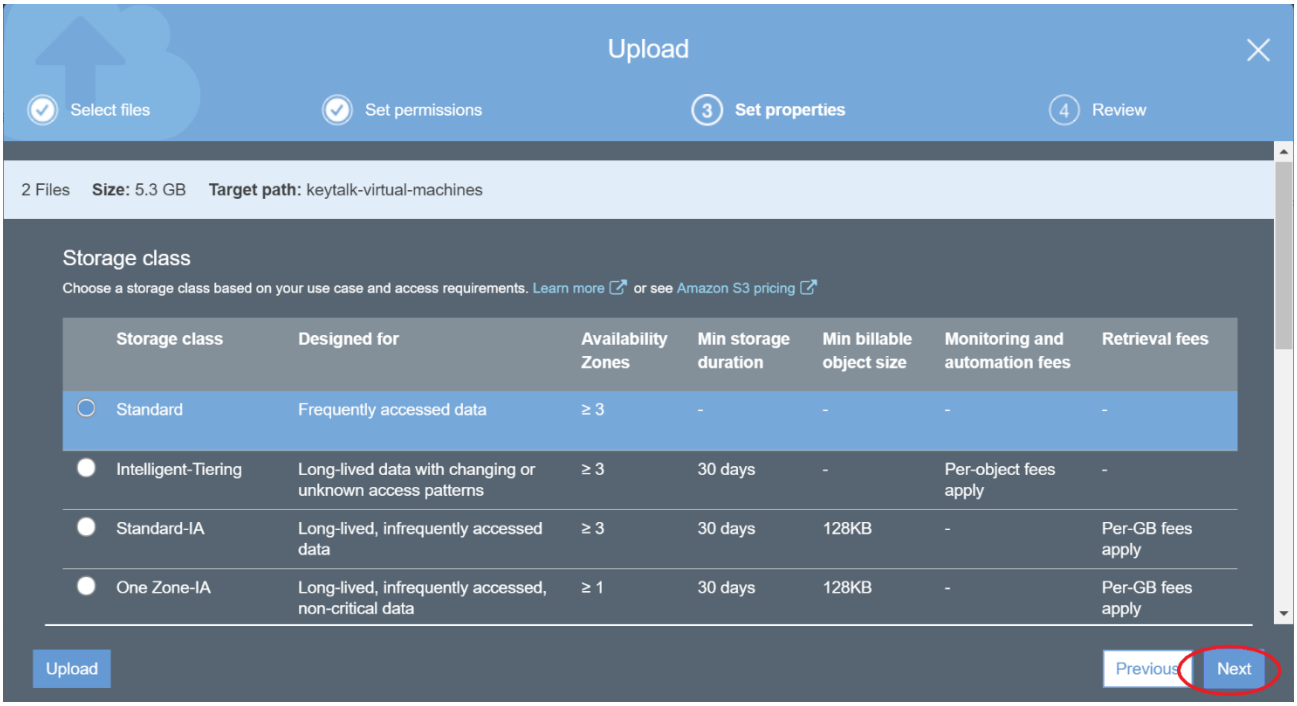


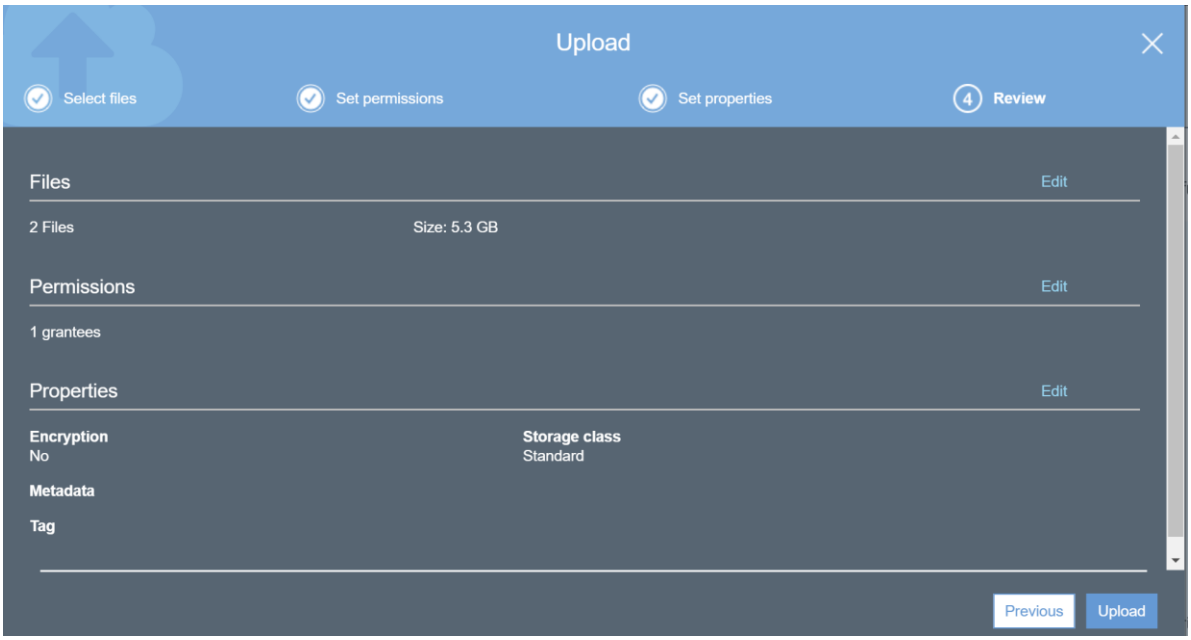

Upload
1 Select files
2 Set permissions
3 Set properties
4 Review
To upload a file larger than 80 GB, use the AWS CLI, AWS SDK, or Amazon S3 REST API. Learn more
Drag and drop files and folders here
OR
Add files
Upload
Next

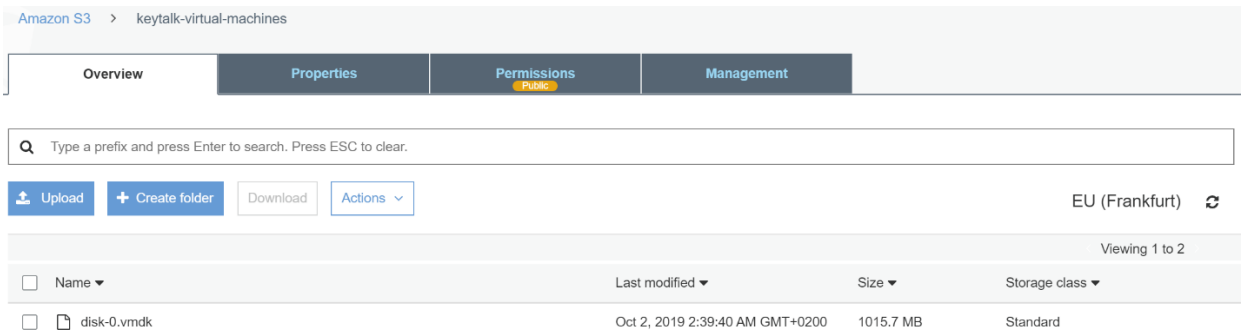

1 Select files
2 Set permissions
3 Set properties
4 Review
1 Files Size: 1015.7 MB Target path: keytalk-virtual-machines
To upload a file larger than 160 GB, use the AWS CLI, AWS SDK, or Amazon S3 REST API. Learn more
+ Add more files
disk-0.vmdk
- 1015.7 MB
Upload
Next


Upload
Select files
2 Set permissions
3 Set properties
4 Review
Manage users
User ID
Objects
Object permissions
info(Owner)
Read
Read
Write
Access for other AWS account
+ Add account
Account
Objects
Object permissions
Manage public permissions
You can't grant public access because Block public access settings are turned on for this bucket. To determine which settings are turned on, check your Block public access settings.
Do not grant public read access to this object(s) (Recommended)
Upload
Previous
Next

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

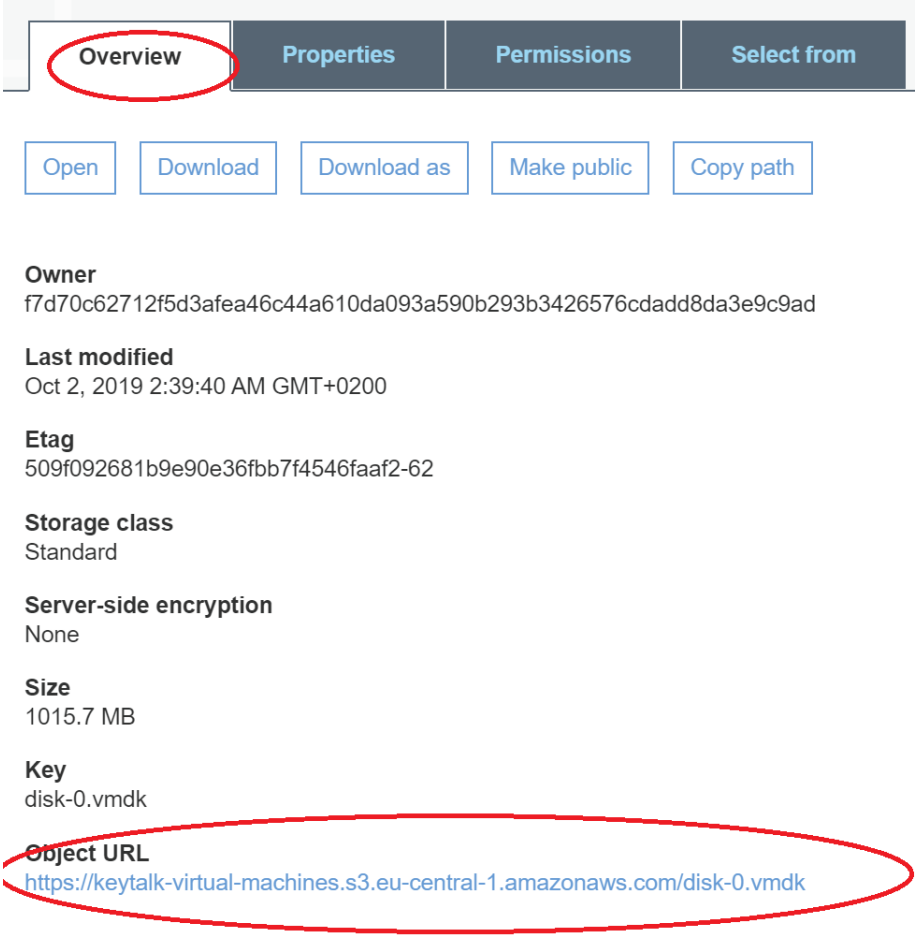






Step 6: Lookup and note down the VMDK Object url.

Select the vmdk file and open the OVERVIEW tab:



Step 7: Create an AWS administrator IAM user under:

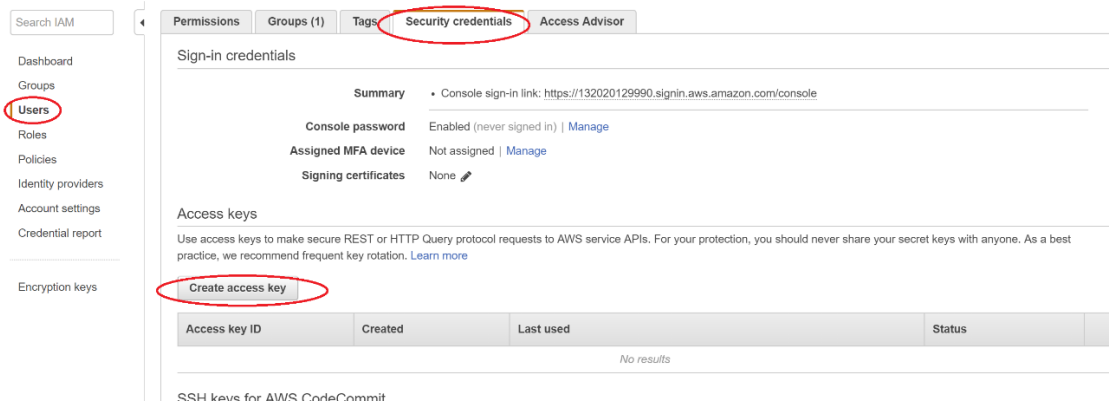
https://console.aws.amazon.com/iam/

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**



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>

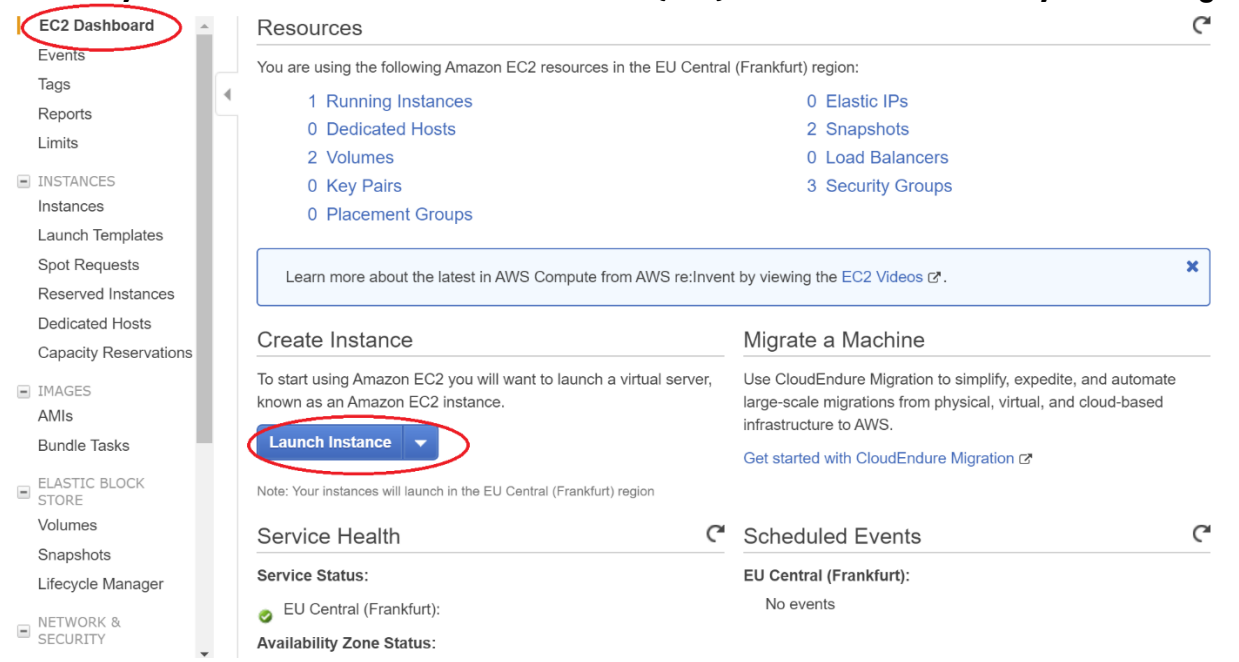
given the above example the command is:

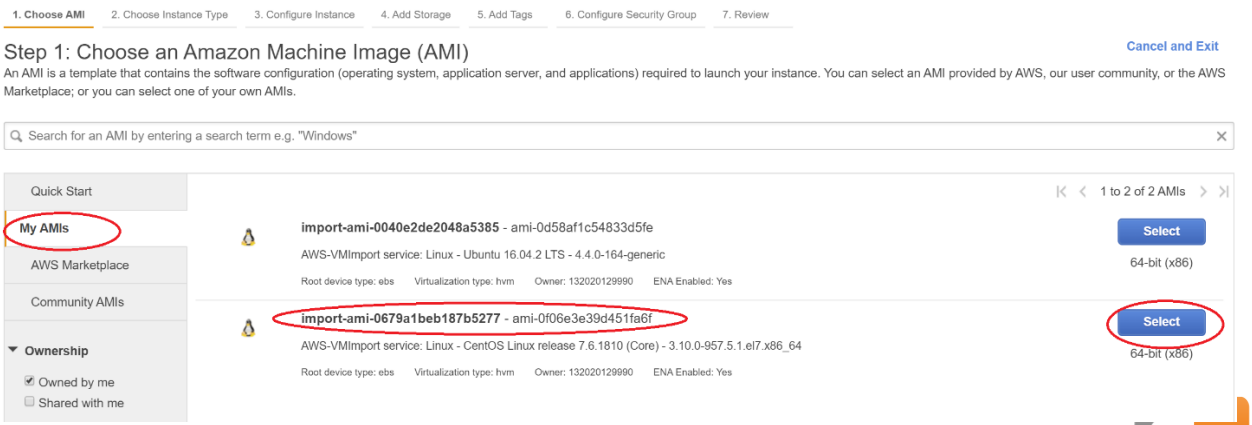
aws ec2 describe-import-image-tasks --import-task-ids import-ami-0679a1beb187b5277

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

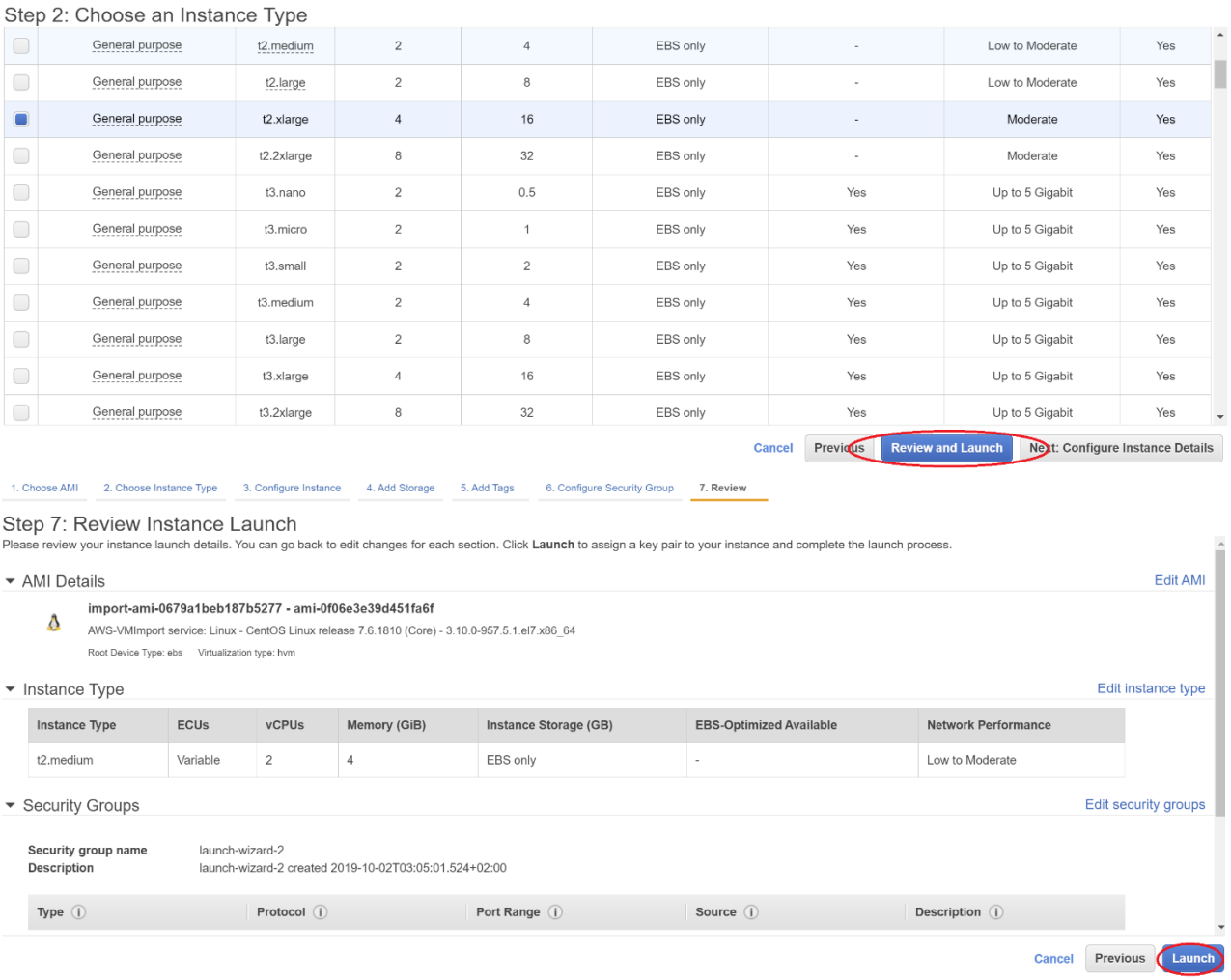
```
C:\aws>aws ec2 describe-import-image-tasks --import-task-ids import-ami-0679a1beb187b5277
{
    "ImportImageTasks": [
        {
            "Architecture": "x86_64",
            "Description": "KeyTalk LDAP VMDK",
            "ImageId": "ami-0f06e3e39d451fa6f",
            "ImportTaskId": "import-ami-0679a1beb187b5277",
            "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"
        }
    ]
}

C:\aws>
```

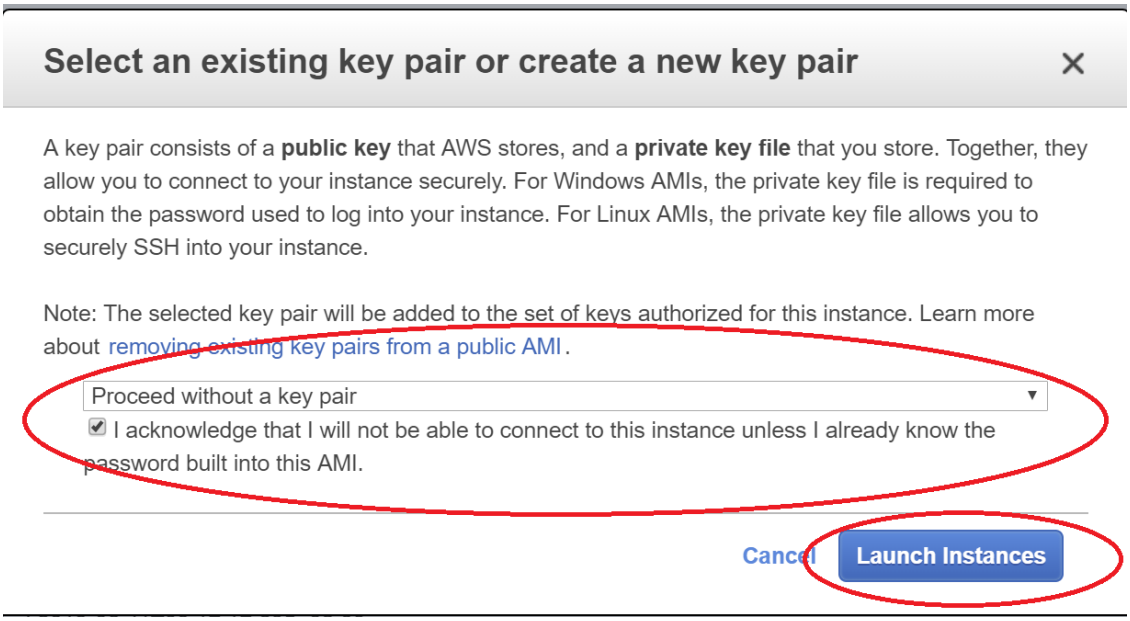
Step 14: Launch your created Amazon Machine Instance (AMI) as an EC2 Instance for your AWS region:





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)

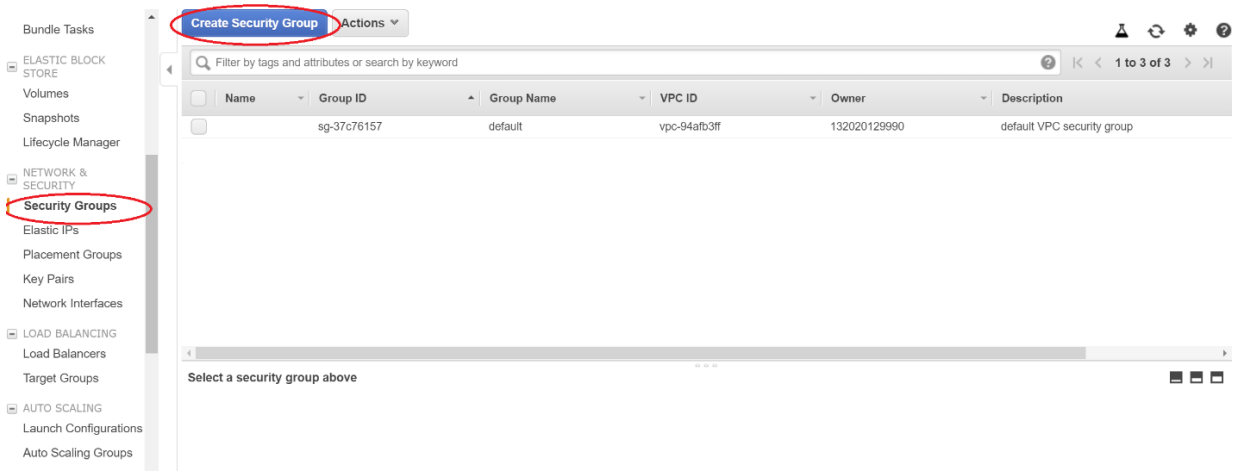


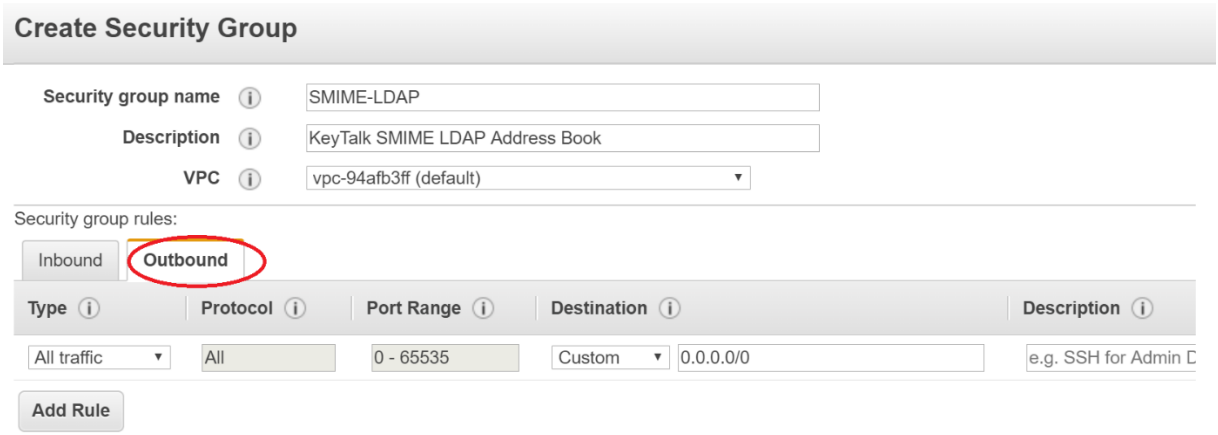


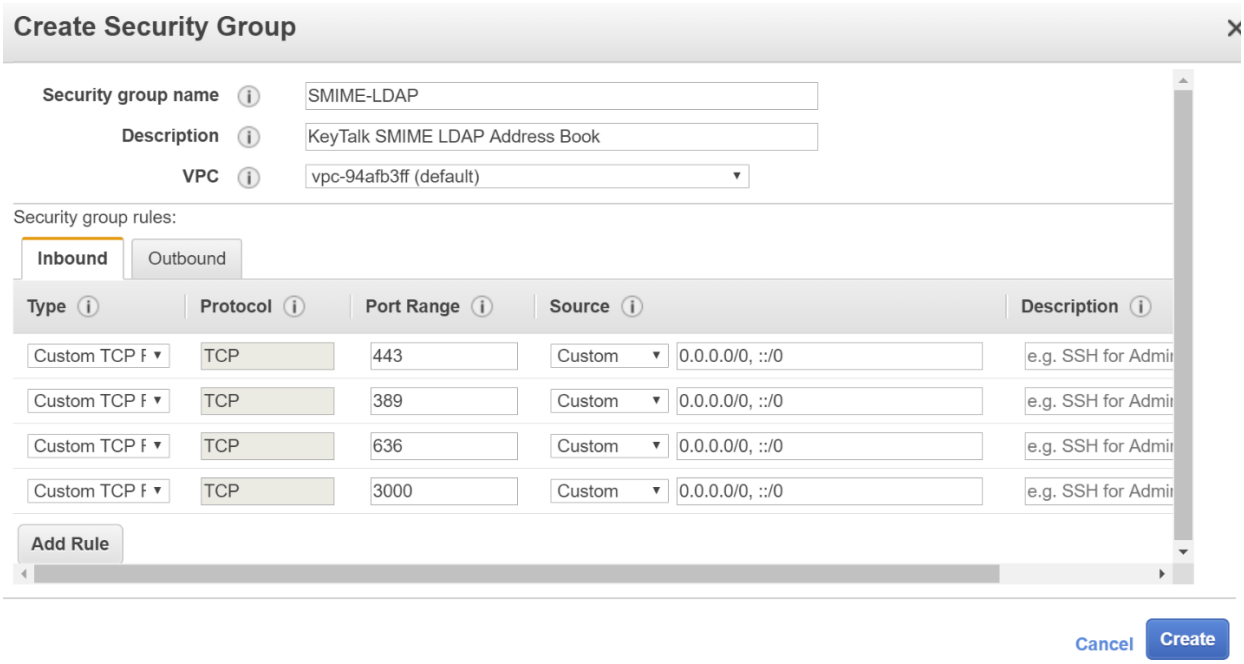
Possibly the instance will not launch as your account first needs a verification by AWS based on your chosen region.

Step 15: Set the Security policy firewall rules and inbound ports

Go to EC2 Security Groups, and select either edit existing or create new:

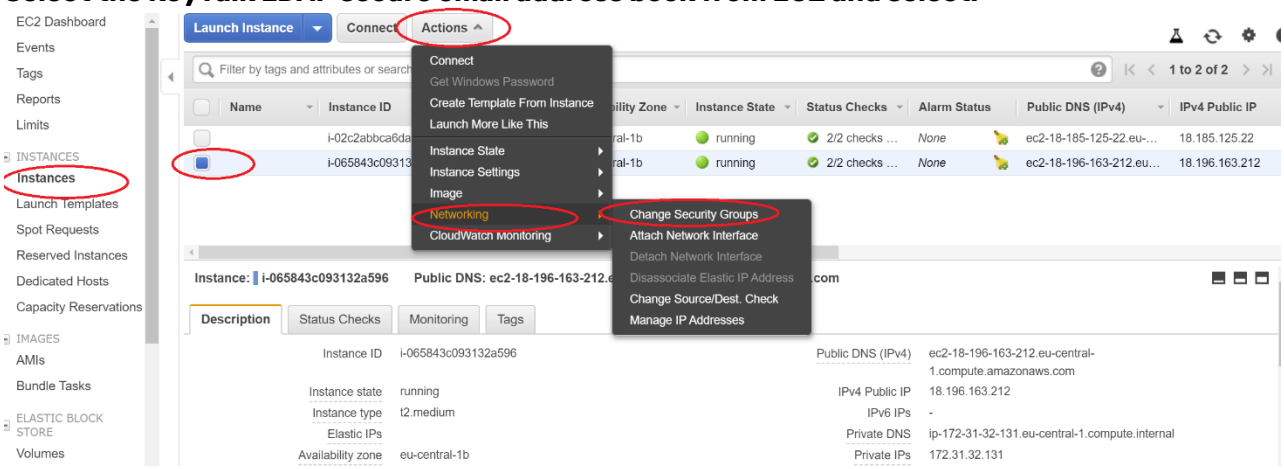




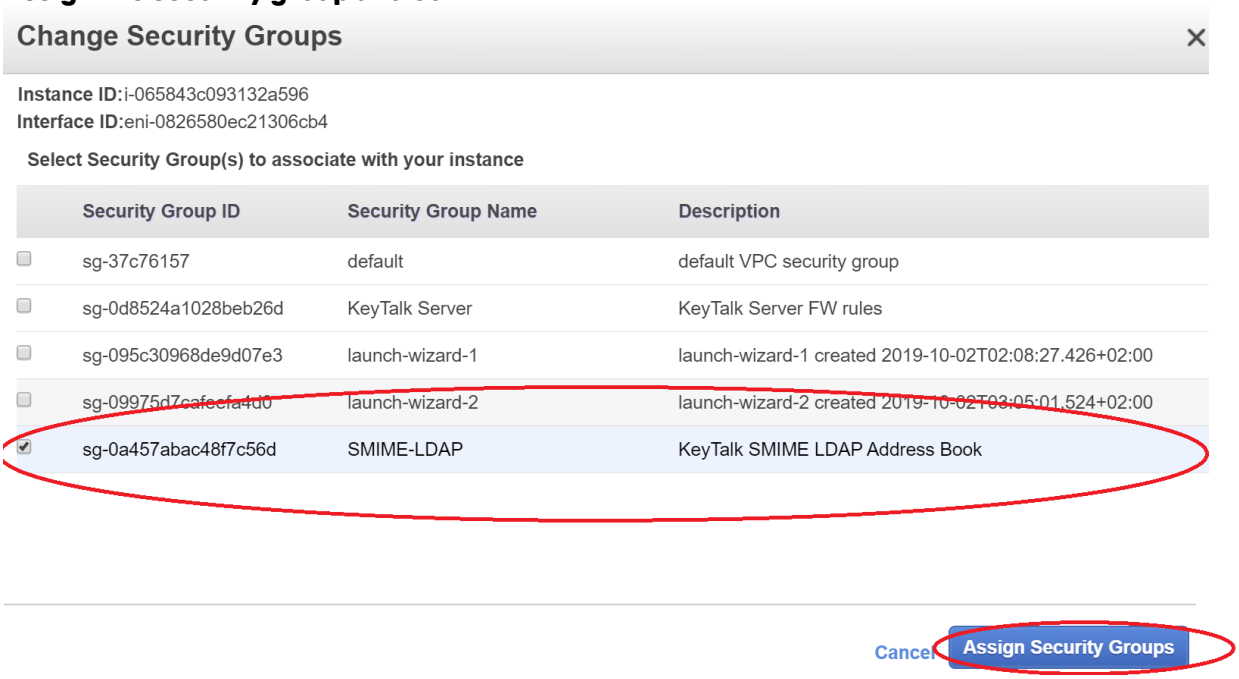


Step 16: Apply the security group:

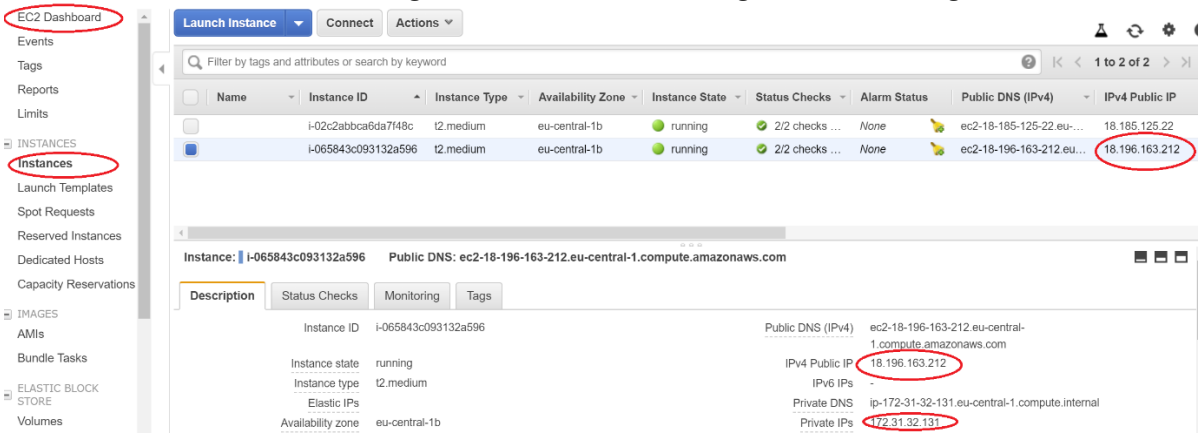
Select the KeyTalk LDAP secure email address book from EC2 and select:



Assign the security group and confirm:



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

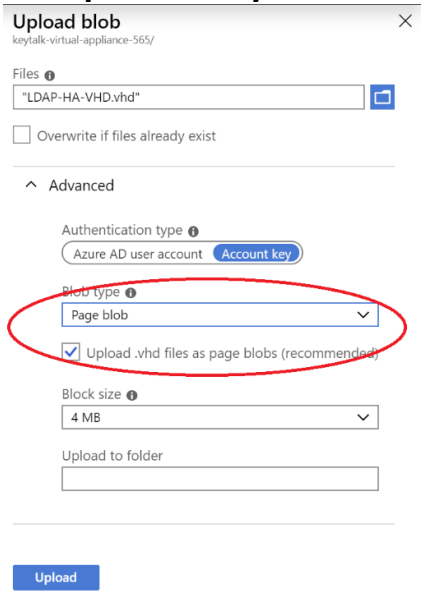


ANNEX B: Importing KeyTalk LDAP virtual appliance in Azure

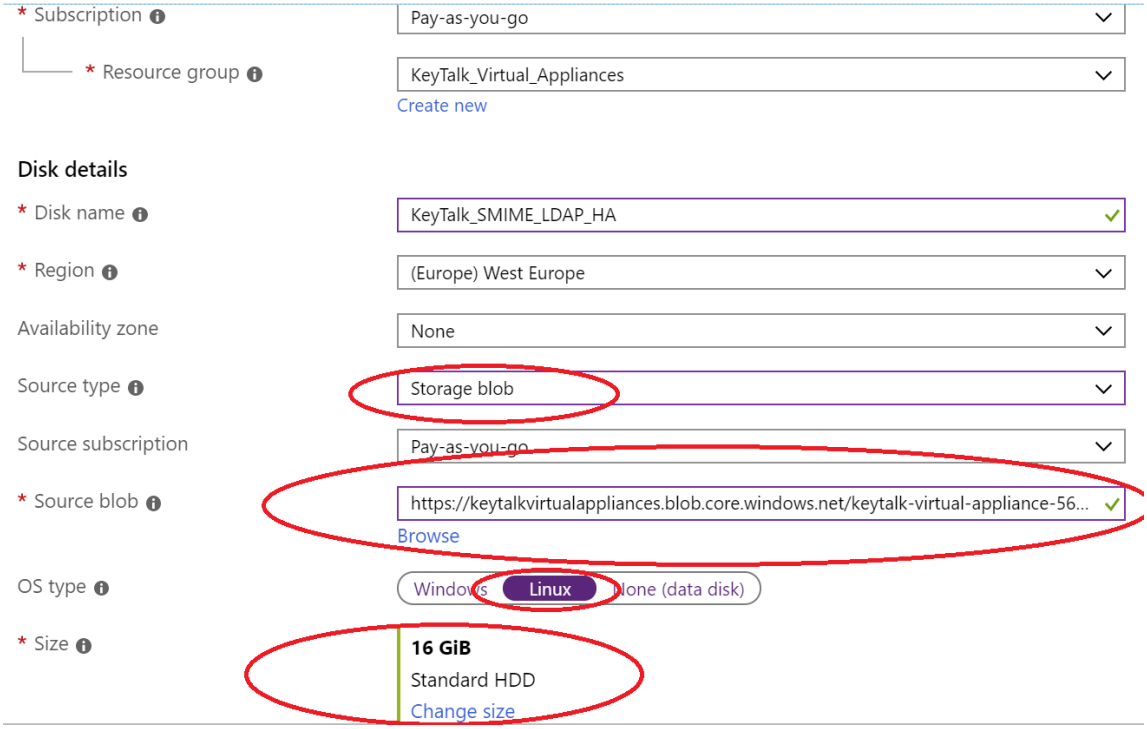
Step 1: Download the KeyTalk virtual appliance for Hyper-V / Azure from the KeyTalk website download section.
OR use the pre-uploaded public available Azure Blob as found here:
https://keytalkvirtualappliances.blob.core.windows.net/keytalk-virtual-appliance-565/LDAP-HA-VHD.vhd
and continue with step 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"

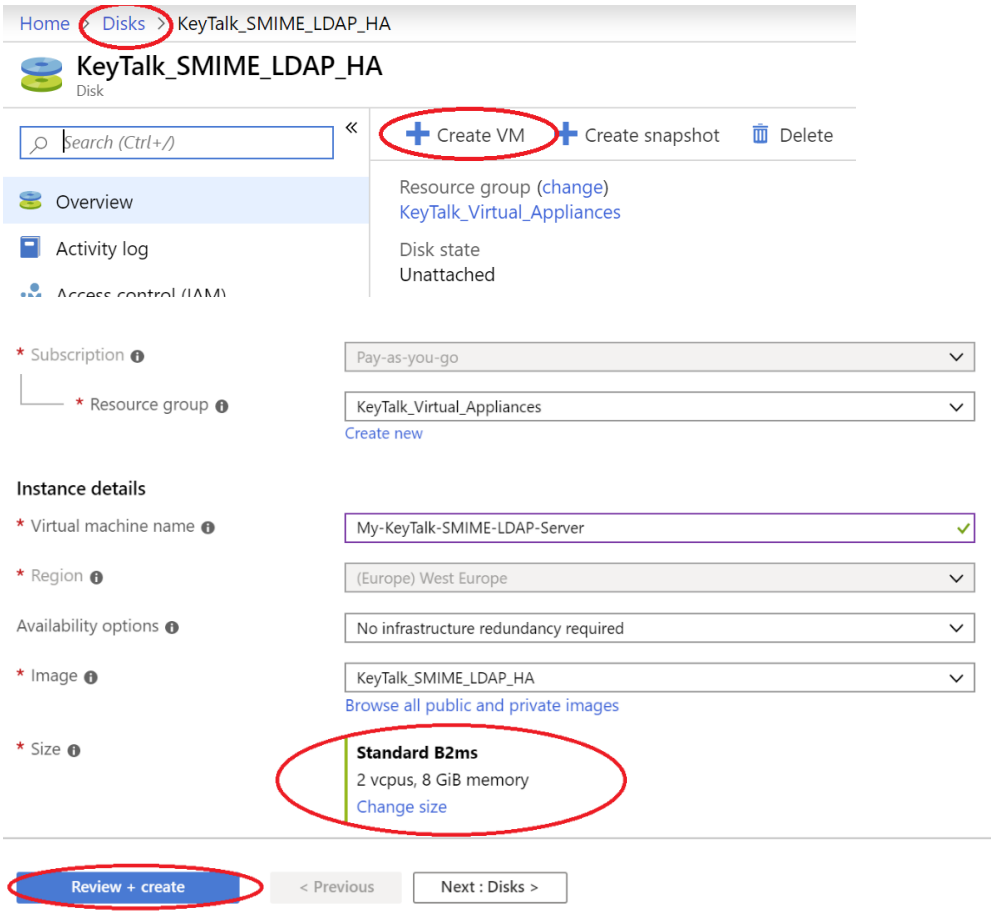


Step 4: After the upload go to Azure Portal -> Disks -> ADD and select the uploaded VHD



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



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)