KeyTalk Firmware 4.3.3

Administrator Appliance Manual:

Installation and settings

This document is propriety of KeyTalk BV. This is a controlled document; it may be copied and distributed through other channels, but nothing in it may be changed without knowledge and consent of KeyTalk BV or its operational branch KeyTalk 1 BV.

The information in this document is subject to change without notice.

KeyTalk BV assumes no liability for any damages incurred, directly or indirectly, from any errors, omissions or discrepancies between the software and the information contained in this document.

KeyTalk is a registered trademark and the KeyTalk logo is a trademark of KeyTalk BV.

Document name:	KeyTalk Administrator manual
Version:	4.3.03
Date:	27-Oct-14

Document control

Document information	
Author	Michael van der Sman
Owner	KeyTalk BV
Document Version	4.3.03
Document status	Final

Revision # & Date	Summary of Changes
4.002 22 Jun 11	Initial release
4.003 13 Jul 11	Added chapter on LCD display, updated Remote Exit chapter
4.004 25 Jul 11	Additional information added on HAD chain
4.005 16 Aug 11	Updated chapters: 5/12.2/13/15/17/19/21.3/21.4/21.5/22.1/22.2/ 23.1.2.2/23.1.2.3/23.2.2.2/27 Added chapters: 2.1
4.101 23 Jan 12	Updated screenshots, TrustAlert brand replaced with Elephant Security, updated chapters 17, 21, 23, 25, 27
4.102 17 Feb 12	Updated chapters 25.2 to 25.6
4.2 – 19 Jun 12	Update to KeyTalk Firmware version 4.2 Replaced the product name KeyTalk with KeyTalk. This change in name has not yet been realized in the software.
4.201 – Aug 2012	Language edited; updated screenshots added; rewrote chapter 22.
4.202 – 12 July 13	Updated brand to KeyTalk
4.301 – 11 Oct 13	Updated to KeyTalk Firmware version 4.3
4.3.3 – 27 Feb 14	Updated to KeyTalk Firmware version 4.3.3

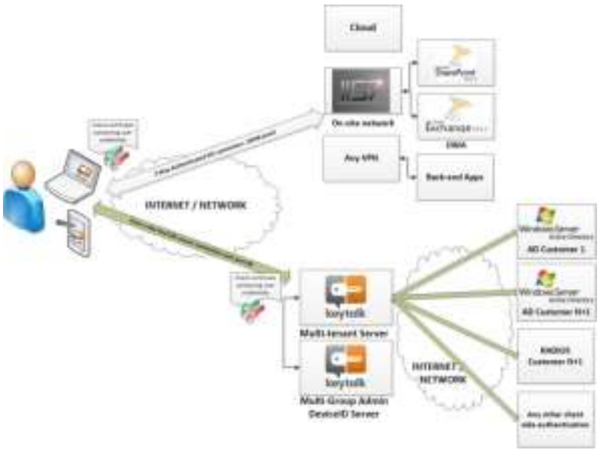
Table of contents

1. Introduction

Thanks for choosing KeyTalk. This product has been designed to make safe communication a reality. On top of that KeyTalk has many additional benefits.

With our patented KeyTalk technology, you can easily provide your entire user community, whether internal or external, with on demand short lived X.509 certificates.

All built upon your existing infrastructure, so there is no need to change backup procedures, or to teach your community of users new authentication methods.



The KeyTalk appliance simply makes it happen.

KeyTalk provides you with advanced features, which make your life as a user easier and more secure when making use of your company's or partner's online environment.

Common usages:

- Single Sign-On to web-based environments
- Digital signing of internal documents
- Highly secure connections to network-based environments
- Protection of your authentication credentials and data-in-motion against Man-in-the-Middle intrusions
- Optionally binding the trusted computer device(s) to the user or company community, allowing for Multi-Factor-Authentication

X.509 user certificates have been the standard since 1988, and are commonly accepted by all Operating Systems. As a result not only do these user certificates enable you the highest level of **safe encrypted communication**, as well as many **more features** with the same ease of management, such as:

- Single Sign-On for certificate aware applications
- Federated Identity

- 802.1x EAP/TLS

Certificates issued by the KeyTalk appliance work natively with all major network and client brands, such as, but not limited to:

- CISCO
- Juniper
- F5
- Fortinet
- CheckPoint
- Palo Alto
- HP
- Huawei
- Microsoft
- Adobe
- SAP
- IBM
- Oracle
- Novell
- Google
- OpenVPN

KeyTalk is a product which seamlessly fits into your existing network infrastructure. In a highly secure manner, it automatically creates, distributes, and (de)installs, short lived X.509v3 user certificates on the user's device, for the primary purpose of user credentialing and secure access control.

X.509 is the industry standard since the 80's and is supported by all major network components and enterprise application solutions, and is now made available for short lived certificates, making it the perfect unified access control solution. Managing X.509v3 certificates has thus far been one of the greatest cost factors in high secure environments. Cost is now minimized as a direct result of short lived certificates, making administrative efforts on Certificate Revocation Lists obsolete.

By re-using your existing authentication environment, optionally leveraging it with trusted corporate hardware recognition, reducing the lifecycle of the certificate, and ultimately automating the certificate requests, creation, distribution and (de)installation, certificate management has become easy as pie with our KeyTalk product.

To summarize:

KeyTalk protects your data in motion by providing secure access for machine-to-machine communication and data transmissions between devices, corporate networks and cloud applications. It prevents common intrusions such as Man-in-the-Middle.
KeyTalk generates, distributes and installs short lived client certificates on the client device in a fully automated manner, leveraging your existing authentication methodology. Optionally it uses the device hardware characteristics to strengthen the authentication process.

1.1. Getting started

In the following subsections the KeyTalk product is described.

1.2. Installation

All our products are delivered with an Installation manual. This manual provides instructions for installing and de-installing the KeyTalk software and gives an overview of the system requirements necessary to run the software. More detailed technical requirements can be found in the Prerequisites and Technical requirement documents.

1.2.1. Using the software

How to use KeyTalk products and an explanation of terminology and icons used in the software are described in detail in the User manual. Next to describing the hardware, the functionalities of the software are also described in full detail. In case of product upgrades an overview of the new functionalities is incorporated in the User manual as well as listed in the product's Release Notes.

Please consult your KeyTalk supplier or partner for more information.

1.2.2. Support

In case you encounter issues when using our products, please contact your KeyTalk supplier or partner. Contact details have been made available to you directly by our partner.

KeyTalk also has a service desk reachable 24/7. They primarily provide 3rd line support (i.e. bug fixes). They can be contacted by e-mail or telephone.

Contact details KeyTalk Service desk 3rd line only

E-mail: support@keytalk.com

More: http://www.keytalk.com/pages/contact.php

1.3. System configurations

You can have one or more KeyTalk (virtual) appliances configured in **high availability** mode.

1.3.1. Optional configurations

KeyTalk can be used in combination with KeyTalk’s DevID (virtual) appliance.

Within an organization DevID allows the binding up to 10 different hardware signatures of a user’s devices to a single unique user. All is done according to the offered authentication service. DevID can be set to automatically learn up to the maximum number of hardware signatures that is allowed per user (setting).

Moreover, DevID is multi-tenant, allowing multiple user groups to be defined per specific KeyTalk authentication services. Each user-group can be separately managed by one or more service operators each with its own authorization, allowing one to deploy and manage DevID in a very flexible manner. This way, your Admins do not have to do all the work by themselves.

2. Front Panel Components

This section does not apply for the virtual version of KeyTalk

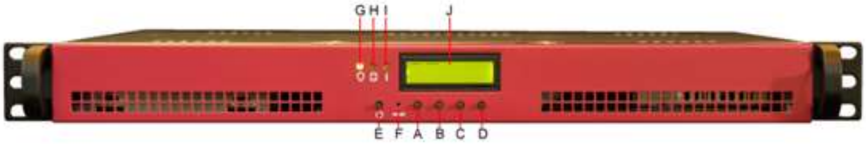


Figure 1: Front panel KeyTalk (color of front bezel may vary)

	Component	Description
A	Display navigation button A	Controls the navigational controls for the LCD information menu (see section 24 'LCD information display').
B	Display navigation button B	Controls the navigational controls for the LCD information menu (see section 24 'LCD information display').
C	Display navigation button C	Controls the navigational controls for the LCD information menu (see section 24 'LCD information display').
D	Display navigation button D	Controls the navigational controls for the LCD information menu (see section 24 'LCD information display').
E	Power button	Press to start the device when switched off. Press and hold for several seconds to switch off the appliance.
F	RESET button	Press (using a paperclip) and hold for several seconds to stop the device. The RESET button only needs to be used when normal switch off using the Power button is not working.
G	Power indicator	Lights up when the power is switched on.
H	Disk indicator	Data is stored on the Solid State Disk. When this indicator flashes the Solid State Disk is active.
I	Information indicator	Lights up when important messages require your attention.
J	LCD Display	Displays the state the device is in and displays menu items for local administration.

Do not replace any components as this will void your KeyTalk warranty.

***Note:** replacing hardware components will result in malfunctioning of the system.*

3. Back Panel Components

This section does not apply for the virtual version of KeyTalk

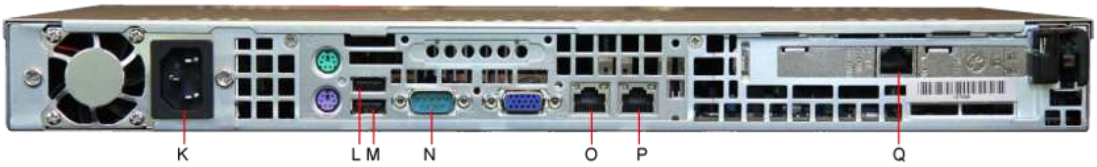


Figure 2: Back panel KeyTalk

	Component	Description
K	Power port	Connector port for the power cable.
L	USB port 1	It is possible to perform functional upgrades via a USB key using this USB port.
M	USB port 2	It is possible to perform functional upgrades via a USB key using this USB port.
N	RS232 port	Manufacturer trouble shooting connector.
O	Network Interface Connector (NIC)	For connection to other KeyTalk appliances in high availability mode, including DEVID. The default IP for this connector is 172.16.1.1.
P	Network Interface Connector (NIC)	For connection to the local management device. The default IP for this connector is 10.1.1.1.
Q	Network Interface Connector (NIC)	For connection to the external network. The default IP for this connector is 192.168.1.1.

Do not replace any components as this will void your KeyTalk warranty.

***Note:** replacing hardware components will result in malfunctioning of the system.*

4. Top Panel Components

This section does not apply for the virtual version of the KeyTalk appliance

On the top panel of the appliance, between the front bezel and the appliance top cover, you will find a blue label.

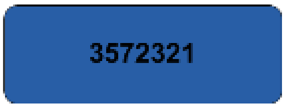


Figure 3: Blue label with appliance's tamper evident serial number

This security label displays the unique appliance tamper evident serial number and should not be removed. It is used for identification purposes in case support is requested.

Removing or otherwise manipulating this label will cause the label to permanently change. KeyTalk advises you to check this label on a regular basis to make sure it is undamaged. Should the label be damaged, please contact your KeyTalk supplier who can provide you with a new label.

In case the label is damaged without your knowledge, be warned that your KeyTalk appliance may have been opened and tampered with. Please report such incident to your KeyTalk administrator and/or security officer.

When the device needs to be sent to the manufacturer for repair, open the device by breaking the label and remove the hard disk. This hard disk contains your company data and should not be sent to the KeyTalk partner or the KeyTalk manufacturer. When the device has been repaired, you will receive it back with a new hard disk and label. This hard disk will be in the initial state. Your settings and company data can be restored from a backup. Please refer to the 'Backup and Restore' section for more information on how to do this. The replacement harddisk or repair can result in additionally invoiced cost.

5. Quick Start Guide

Assumptions:

- The KeyTalk appliance is by default delivered in DEMO configuration and should work immediately after applying the configurations described below.
- For this quick start configuration the default Windows KeyTalk Client should be used together with the DEMO RCCD file. (RCCD: Readable Client Configuration Data)
- For security reasons the DEMO key and certificate material must always be replaced with production material before taking the solution into a production state and environment.
- When using production keys and certificate material, a corresponding production KeyTalk client RCCD file must be used, otherwise communication will fail. An RCCD file can be generated by your organization. This functionality is described in Chapter 5 of the Client Administrator Manual.
- DNS, NTP, HTTP, HTTPS, SysLog, port 3000, and optionally icmp ping 0,8 are assumed to be available for connection purposes.

5.1. Step 1: Powering the physical appliance

a) Remove the appliance from its box.
b) Plug the black power cord into the appliance back power-port ‘K’.
c) Plug the power cable into a power socket-connector.
d) Press the power-on button (button ‘E’).

5.2. Step 2: Connecting the appliance to the internal network

The KeyTalk appliance has 3 active Network Interface Connectors (NIC) ‘O’, ‘P’ and ‘Q’ in Figure 2: Back panel KeyTalk.

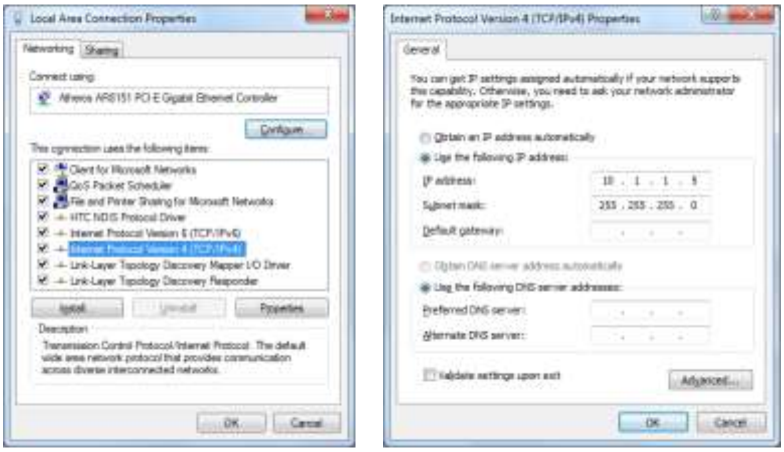
The NIC ‘P’ is 10.1.1.1 and is assigned to the KeyTalk management interface. This NIC should only be accessible to the system administrator.

e) Connect the administrator PC/Laptop by UTP cable.

f) Configure the administrator PC/Laptop to the 10.1.1.x network so that you may be able to connect to 10.1.1.1.
Pick for example the 10.1.1.50 address (address must be 10.1.1.x with x>4) for the administrator PC and use network mask 255.255.255.0.

NOTE: By default pre-configuration is based on IPV4, however IPV6 is fully supported. The focus for manuals and training is, however, on IPV4 and will not go into detail for IPV6 configuration.

Sample screenshots on a Windows 7 (64) PC on how to configure your IP:



Local Area Connection Properties

Connect using: Atheros AR8151 PCI-E Gigabit Ethernet Controller

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ HTC NDIS Protocol Driver
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Description: Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

Internet Protocol Version 4 (TCP/IPv4) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:
IP address: 10 . 1 . 1 . 5
Subnet mask: 255 . 255 . 255 . 0
Default gateway: . . .

○ Obtain DNS server address automatically
● Use the following DNS server addresses:
Preferred DNS server: . . .
Alternate DNS server: . . .

□ Validate settings upon exit

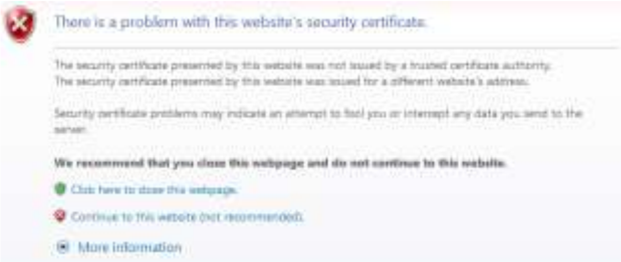
Figure 4: IP configuration on a Windows 7 (64bit) PC

5.3. Step 3: Connecting to the appliance administrator interface

The KeyTalk appliance Graphical Admin Interface can be accessed by browser over the following URL: https://10.1.1.1:3000.
Note: Pay attention to the S in HTTPS and port 3000!

Because the appliance is configured using a self-signed SSL certificate by default, you will likely get a warning that the security certificate was not issued by a trusted certificate authority.

In this case, ignore the warning and continue to the website. This is a workaround!!; a trusted certificate should be obtained from a known certificate authority such as VeriSign, GoDaddy and Cybertrust, or from the KeyTalk Certificate Authority, before going into production. When the certificate is installed, no warning should occur.



There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website was issued for a different website's address.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.
Continue to this website (not recommended).
More information

Figure 5: Sample warning

You will then go to the admin login page for KeyTalk.

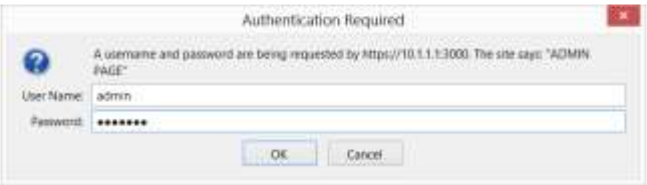
NOTE: When running the virtual appliance, it may not be possible for you to reach the 10.1.1.1:3000 address due to your used subnet. In this case kindly refer to [chapter 6.1](#)

5.4. Step 4: Authenticating to the administrator interface

The default authentication credentials to access the KeyTalk administrator interface role are:

User: admin

Password: change!



A username and password are being requested by https://10.1.1.1:3000. The site says: "ADMIN PAGE"

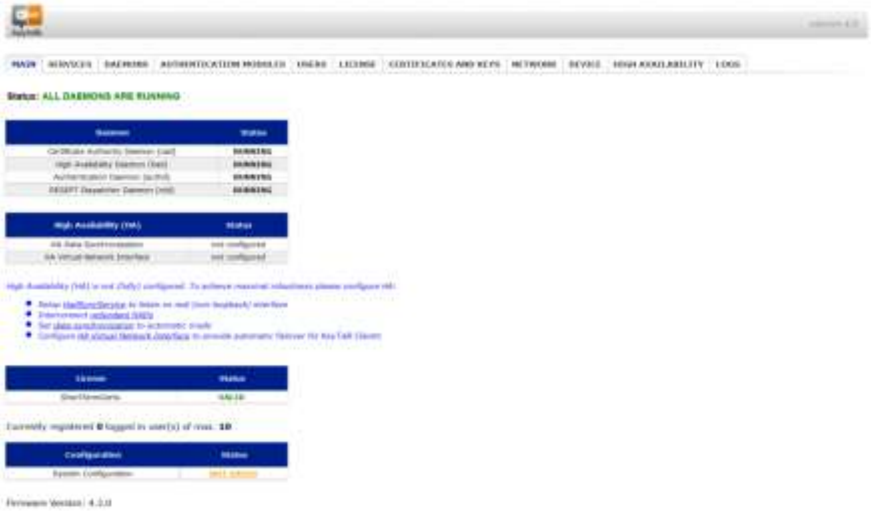
User Name: admin

Password: ••••••••

Figure 6: Login to KeyTalk administration page after ignoring the certificate warning

This user has full access to all the options on the KeyTalk device.

The homepage of KeyTalk will open:



Status: ALL DAEMONS ARE RUNNING

Daemon	Status
Certificate Authority Daemon (cad)	RUNNING
High Availability Daemon (had)	RUNNING
Authentication Daemon (authd)	RUNNING
RESEPT Dispatcher Daemon (rdd)	RUNNING

High Availability (HA)	Status
HA Data Synchronization	not configured
HA Virtual Network Interface	not configured

High Availability (HA) is not (fully) configured. To achieve maximal robustness please configure HA:

- Setup HaSyncService to listen on real (non loopback) interface
- Interconnect redundant RASs
- Set data synchronization to automatic mode
- Configure HA Virtual Network Interface to provide automatic failover for KeyTalk Clients

License	Status
ShortTermCerts	VALID

Currently registered 0 logged in user(s) of max. 10

Configuration	Status
System Configuration	[illegible]

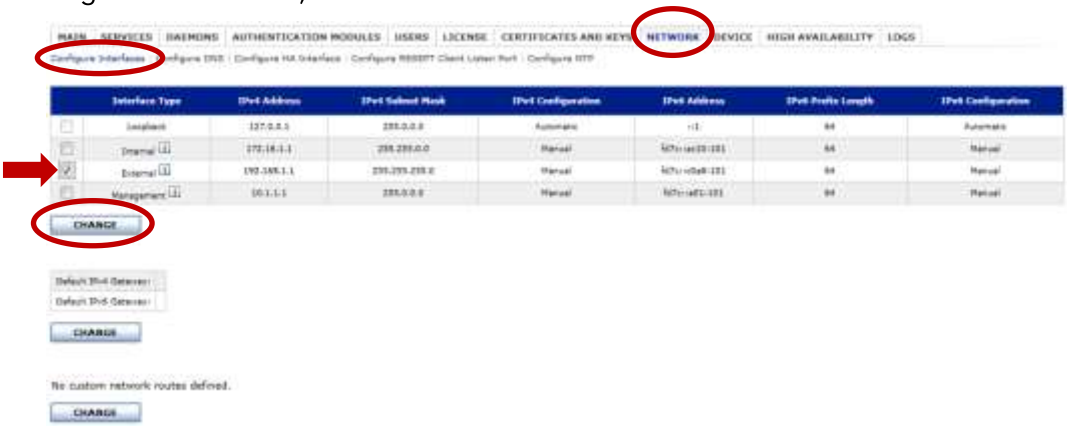
Firmware Version: 4.2.0

Figure 7: Homepage KeyTalk

5.5. Step 5: Set network configuration

For configuring the network, network administration knowledge is required.

To set the network configuration, select the ‘NETWORK’ tab in the upper menu, select “Configuration Interface”, enable the ‘External’ checkbox and select “CHANGE”.



	Interface Type	IPv4 Address	IPv4 Subnet Mask	IPv4 Configuration	IPv6 Address	IPv6 Prefix Length	IPv6 Configuration
☐	Loopback	127.0.0.1	255.0.0.0	Automatic	::1	64	Automatic
☐	Internal	172.16.1.1	255.255.0.0	Manual	fd7c::ac10:101	64	Manual
☑	External	192.168.1.1	255.255.255.0	Manual	fd7c::c0a8:101	64	Manual
☐	Management	10.1.1.1	255.0.0.0	Manual	fd7c::a01:101	64	Manual

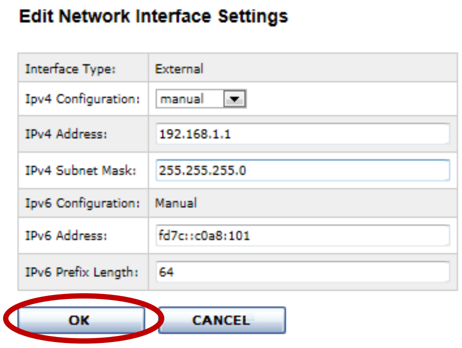
Default IPv4 Gateway:
Default IPv6 Gateway:

No custom network routes defined.

Figure 8: Setting network configuration

5.6. Step 6: Edit network interface settings

Configure ‘IP Address’, ‘Subnet Mask’ and the ‘Default Gateway’ to match your own network topology and click ‘OK’ to save these settings.



Edit Network Interface Settings

Interface Type:	External
Ipv4 Configuration:	manual
IPv4 Address:	192.168.1.1
IPv4 Subnet Mask:	255.255.255.0
Ipv6 Configuration:	Manual
IPv6 Address:	fd7c::c0a8:101
IPv6 Prefix Length:	64

Figure 9: Network Interface Settings

Note: *Optionally you can set a gateway for each NIC separately.*

5.7. Step 7: Change administrator password

To guarantee the best security possible, it is important to change all user passwords before step 10 ‘Connecting the appliance to the external network’.

The Graphical Administrator Interface can be used, when required, for maintenance.

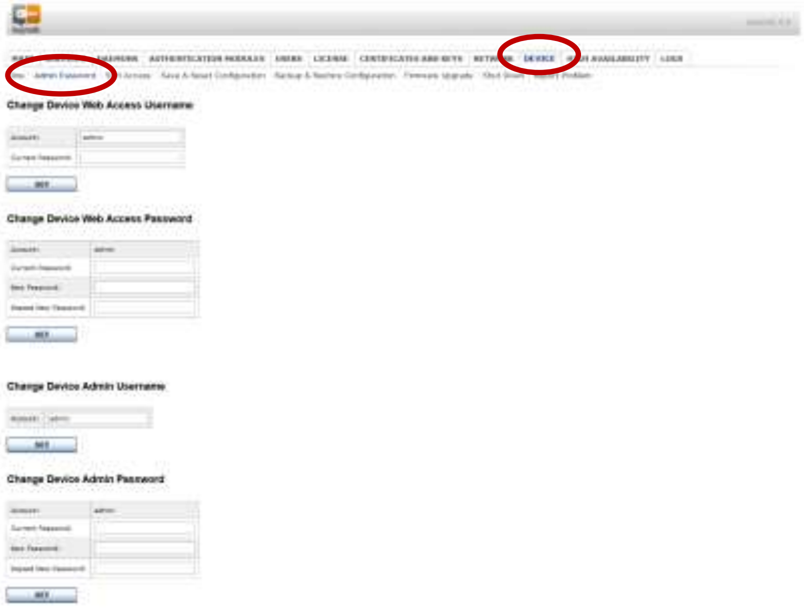
The Admin authentication credentials are by default set to:

Graphical Administrator Interface (Admin GUI):

User:	admin
Password:	change!

In order to change the Graphical Administrator Interface password, do the following:

In the upper menu select the 'DEVICE' tab and select 'Admin Password'.



Change Device Web Access Username

Account:	admin
Current Password:	

SET

Change Device Web Access Password

Account:	admin
Current Password:	
New Password:	
Repeat New Password:	

SET

Change Device Admin Username

Account:	admin

SET

Change Device Admin Password

Account:	admin
Current Password:	
New Password:	
Repeat New Password:	

SET

Figure 10: Changing Graphical Administrator Interface password

Enter both current and new password and confirm the new password in the Change Device Web Access Password fields. Press "OK" to activate the new password.

Note: *It is important to remember this password.*

The KeyTalk appliance also has a more powerful user, the device (SSH) admin, for low level administrator maintenance. This user is not enabled by default. If required, contact your KeyTalk supplier or partner to activate SSH using an updated license file.

5.8. Step 8: DNS & NTP/Date Time customization

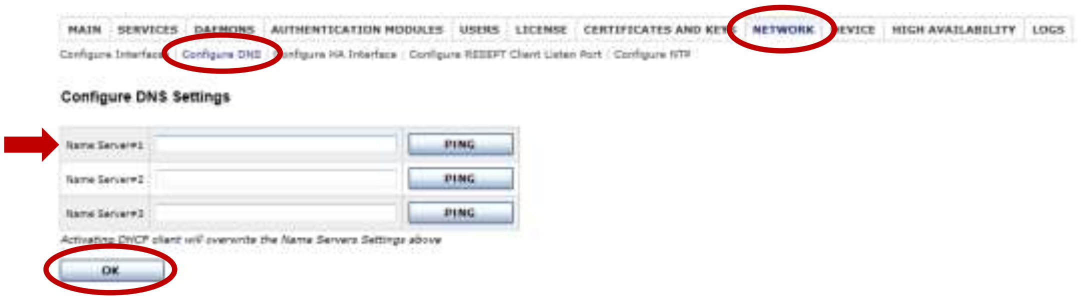
To set your applicable **DNS**, select the "NETWORK" tab in the upper menu and select "Configure DNS".

It is possible to ping the IP in order to check if the IP maps to a live machine.

Note:

The firewall might block the ping (icmp echo request/reply).

Enter the IP addresses of your DNS and select ‘OK’.



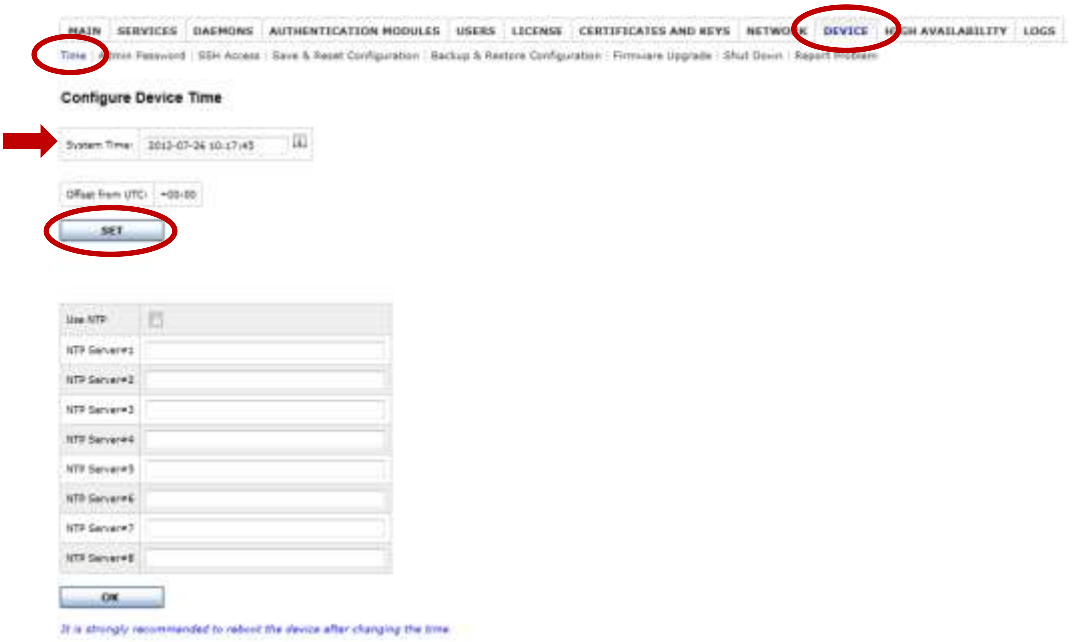
Configure DNS Settings

Activating DHCP client will overwrite the Name Servers Settings above

Figure 11: Setting the applicable DNS

To set the applicable **date/time**, go to the tab “DEVICE” and select “Time”.

Enter the current date and time in UTC(!), and select “SET”.



Configure Device Time

System Time: 2013-07-26 10:17:45

Offset from UTC: +00:00

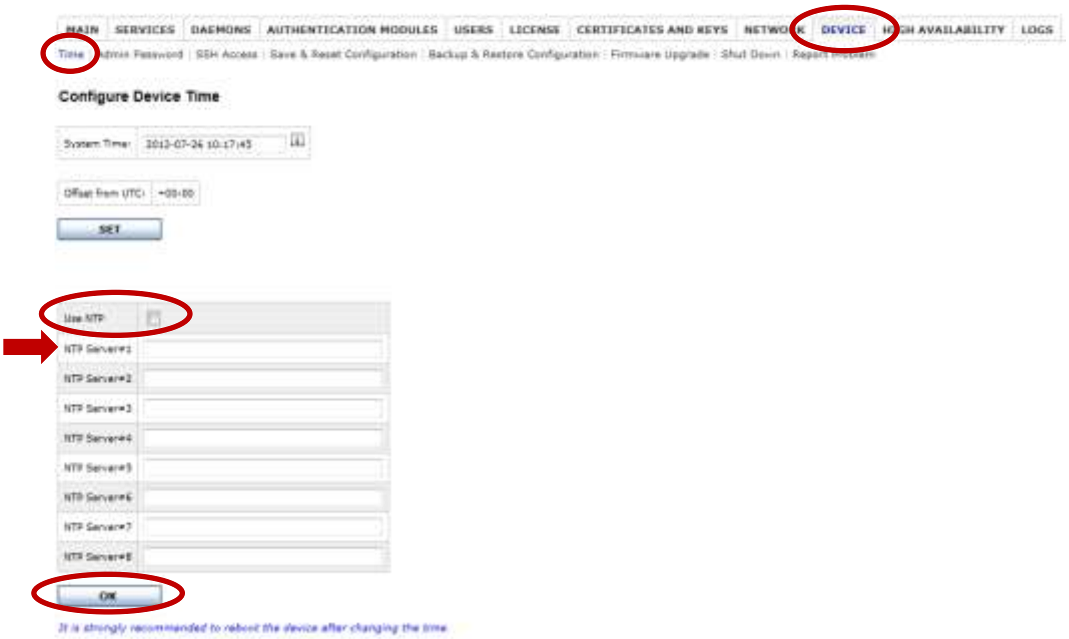
Use NTP □

It is strongly recommended to reboot the device after changing the time

Figure 12: Setting the applicable date/time

***Note:** The Netherlands is UTC+1 (during summertime UTC+2); CST = UTC-6 (during summertime UTC-5); EST = UCT-5 (during summertime UTC-4).*

Preferably set your applicable **NTP server(s)**. When using NTP server(s) also check the ‘Use NTP’ box. Confirm by selecting “OK”.


MAIN
SERVICES
DAEMONS
AUTHENTICATION MODULES
USERS
LICENSE
CERTIFICATES AND KEYS
NETWORK
DEVICE
HIGH AVAILABILITY
LOGS
Time | Admin Password | SSH Access | Save & Reset Configuration | Backup & Restore Configuration | Firmware Upgrade | Shut Down | Report Problem
SET
OK

Configure Device Time

System Time: 2012-07-26 10:17:45

Offset from UTC: +00:00

Use NTP □

NTP Server#1

NTP Server#2

NTP Server#3

NTP Server#4

NTP Server#5

NTP Server#6

NTP Server#7

NTP Server#8

It is strongly recommended to reboot the device after changing the time

Figure 13: Setting your applicable NTP server(s)

Possible problems

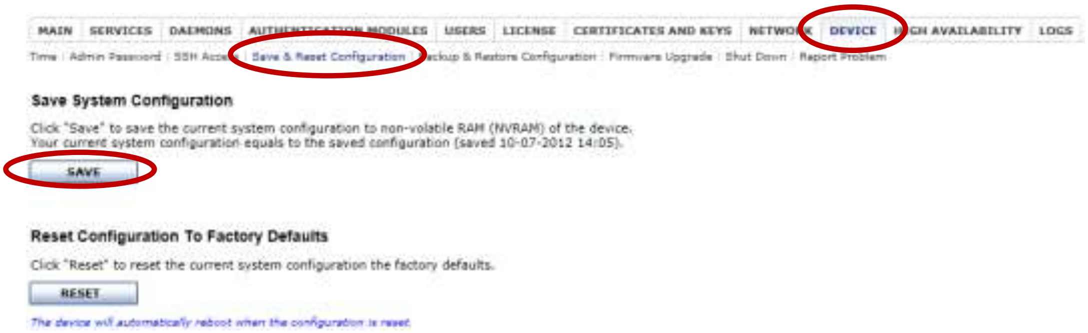
Please make sure the firewall rules allow connection of NTP services (UDP123). Also keep in mind that NTP will only slowly correct the time settings. This is standard NTP behavior and to avoid a delay, manually set the time before enabling NTP. Manually setting the time cannot be done after enabling NTP.

Also see section 14 ‘Date/time & NTP settings’. There are two menu items to configure the time, but both function identically. One menu item is located in the ‘Network configuration’, the other in ‘Device configuration’. Both direct you to the same function.

5.9. Step 9: Save the current configuration

In the main menu select the ‘DEVICE’ tab and select ‘Save & Reset Configuration”.

Select “SAVE” to save the System Configuration.


MAIN
SERVICES
DAEMONS
AUTHENTICATION MODULES
USERS
LICENSE
CERTIFICATES AND KEYS
NETWORK
DEVICE
HIGH AVAILABILITY
LOGS
Time | Admin Password | SSH Access | Save & Reset Configuration | Backup & Restore Configuration | Firmware Upgrade | Shut Down | Report Problem
SAVE
RESET

Save System Configuration

Click "Save" to save the current system configuration to non-volatile RAM (NVRAM) of the device.
Your current system configuration equals to the saved configuration (saved 10-07-2012 14:05).

Reset Configuration To Factory Defaults

Click "Reset" to reset the current system configuration the factory defaults.

The device will automatically reboot when the configuration is reset.

Figure 14: Saving current system configuration

In case a system reboot is necessary the standard configuration will be used unless the changes have been saved. See section 8 'KeyTalk Admin GUI' for details about making changes to the KeyTalk Admin GUI and saving the changes.

5.10. Step 10: Connecting the appliance to the external network

The KeyTalk appliance has 3 active Network Interface Connectors (NIC). These are 'O', 'P' and 'Q' (see section 3 'Back Panel Components').

NIC 'Q' is by default assigned to 192.168.1.1 and to be connected to the external network. This NIC should be used for regular KeyTalk client-server communication.

5.11. Step 11: Testing the KeyTalk solution

Now that the installation is complete, the KeyTalk solution can be tested using the provided demo KeyTalk Client in combination with the DEMO RCCD file.

Update the KeyTalk client configuration: start the KeyTalk Configuration Manager from the Windows START menu:

Figure 15: KeyTalk Configuration Manager in Windows 8

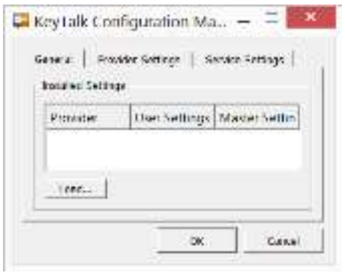


Figure 16: RESEPT Configuration Manager

Load the RCCD file to connect to the KeyTalk appliance by clicking on "Load..."

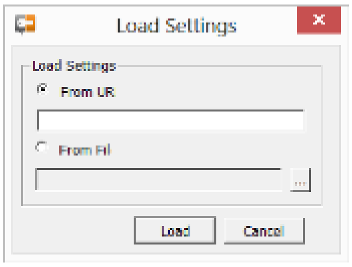
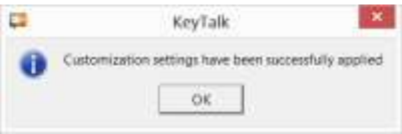


Figure 17: Selecting the setting to load a RCCD file

Browse to the location where the RCCD is saved, either via your browser or from your local system.

Click on “Load” to upload the selected RCCD file. After successful upload the following message will appear on screen:

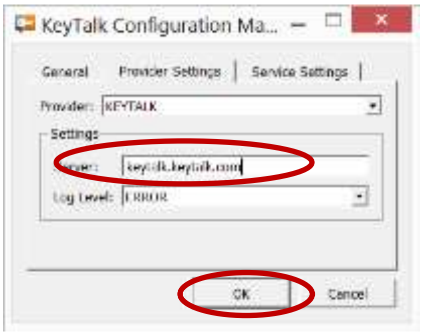


Customization settings have been successfully applied

Figure 18: RCCD file was successfully uploaded and applied

If the screen above does not appear, the RCCD file you tried to upload may be corrupt or hasn’t been signed by KeyTalk’s signingportal. Please recreate the RCCD file and upload again.

Select the “Provider Settings” tab and enter the appropriate KeyTalk Appliance server, which can be specified by IP address or DNS name. When done, select “OK”.



Provider: KEYTALK

Server: keytalk.keytalk.com

Log Level: ERROR

Figure 19: Sample provider settings

For testing purposes the KeyTalk internal user database is already configured with a ‘DemoUser’. Additional users can be easily added using the Admin GUI, see section 19 ‘Authentication modules’ for more information.

NOTE: At the time of writing of this manual, only the Windows client has the option to change the KeyTalk server address. For the mobile clients you need to ensure the RCCD contains the appropriate KeyTalk server address when creating it in the signing portal

Should you be a free trial user, and wish to test also with for example the iOS client, kindly drop us a line by email (support@keytalk.com) and request an updated RCCD file for the demo KeyTalk server and inform us of your preferred KeyTalk server address.

6. IPv4, IPv6 and (virtual) NICs

The KeyTalk appliance fully supports IPv4 and IPv6.

Out-of-the-box demo configurations are based on IPv4.

Admins who wish to make use of IPv6 will need to configure the appropriate IPv6 settings using the graphic user interface of KeyTalk on https://10.1.1.1:3000

6.1. VMWare prompt based IP address changes

In some cases you may be deploying the Virtual Appliance (OVF) directly to your subnet, in which case the default Admin user interface on https://10.1.1.1:3000 might not be available.

You can update the Admin interface IP address by following these easy steps:

a) change /etc/hostname.em2 using the command

```
vi /etc/hostname.em2
```

b) change the default IP and subnet address to what you want to use, and save using the command:

```
:wq
```

c) make the new configuration persistent using the command:

```
/etc/RESEPT/saveconfig.sh
```

d) Now reboot the virtual appliance

6.2. VMWare prompt based changing network interfaces

The KeyTalk appliance by default makes use of 3 (virtual) network interfaces. Each interface segregates specific network traffic using its own built in firewall to prevent bridging of traffic. In some rare cases you may wish to merge these interfaces. To do so follow these steps:

I) Edit the appropriate config file

```
vi /etc/RESEPT/resept.net.conf
```

II) Map the interface you wish to map, taking into account:
em0 – external   em1 – internal   em2 - management
and save using the command:

```
:wq
```

III) make the new configuration persistent using the command:

```
/etc/RESEPT/saveconfig.sh
```

IV) Now reboot the virtual appliance

7. Setting up the appliance

7.1. Powering the physical appliance

1. Remove the appliance from its box.
2. Plug the black power cord into the appliance back power-port (‘K’).
3. Plug the power cable into a power socket-connector.
4. Press the power-on button (‘E’).

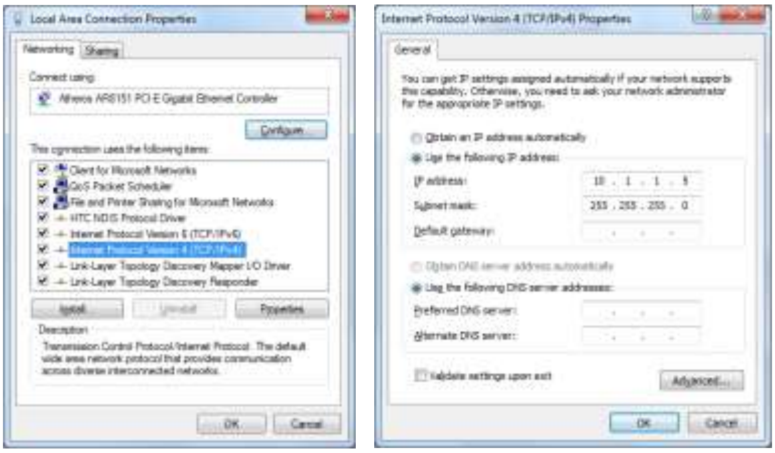
7.2. Connecting the appliance to the internal network

The KeyTalk appliance has 3 active Network Interface Connectors (NIC) (‘O’, ‘P’ and ‘Q’).

The address of ‘P’ is by default 10.1.1.1 and is assigned to the KeyTalk administrator interface.

Follow these steps to connect the appliance to the internal network:

- Connect the administrator PC/Laptop by UTP cable.
- Configure the administrator PC/Laptop to the 10.1.1.0 network so that you are able to connect to 10.1.1.1.
- Sample screenshots on a Windows 7 (64) PC on how to configure your IP from Local Area Connection Properties:



Local Area Connection Properties

Networking | Sharing

Connect using:

Atheros AR8151 PCI-E Gigabit Ethernet Controller

This connection uses the following items:

☑ Client for Microsoft Networks
☑ QoS Packet Scheduler
☑ File and Printer Sharing for Microsoft Networks
☑ HTC NDIS Protocol Driver
☑ Internet Protocol Version 6 (TCP/IPv6)
☑ Internet Protocol Version 4 (TCP/IPv4)
☑ Link-Layer Topology Discovery Mapper I/O Driver
☑ Link-Layer Topology Discovery Responder

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:
IP address: 10 . 1 . 1 . 5
Subnet mask: 255 . 255 . 255 . 0
Default gateway: . . .

○ Obtain DNS server address automatically
● Use the following DNS server addresses:
Preferred DNS server: . . .
Alternate DNS server: . . .

□ Validate settings upon exit

Figure 20: Configure your IP

8. KeyTalk Admin GUI

The KeyTalk appliance Graphic Admin Interface can be accessed with a browser using the following URL: https://10.1.1.1:3000

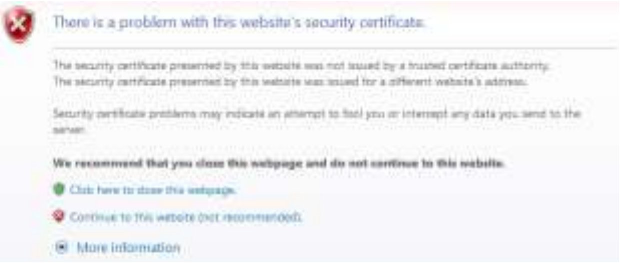
Note: Pay attention to the S in HTTPS and port 3000!

User: admin

The default password was 'change!', but this could have been changed under section 10 'Changing KeyTalk passwords'. Please remember to use your new password.

Because the appliance is configured to use a self-signed SSL certificate by default, you will likely to get a warning that the security certificate was not issued by a trusted certificate authority. In this case, ignore the warning and continue to the website.

Sample warning:



There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website was issued for a different website's address.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.
Continue to this website (not recommended).
More information

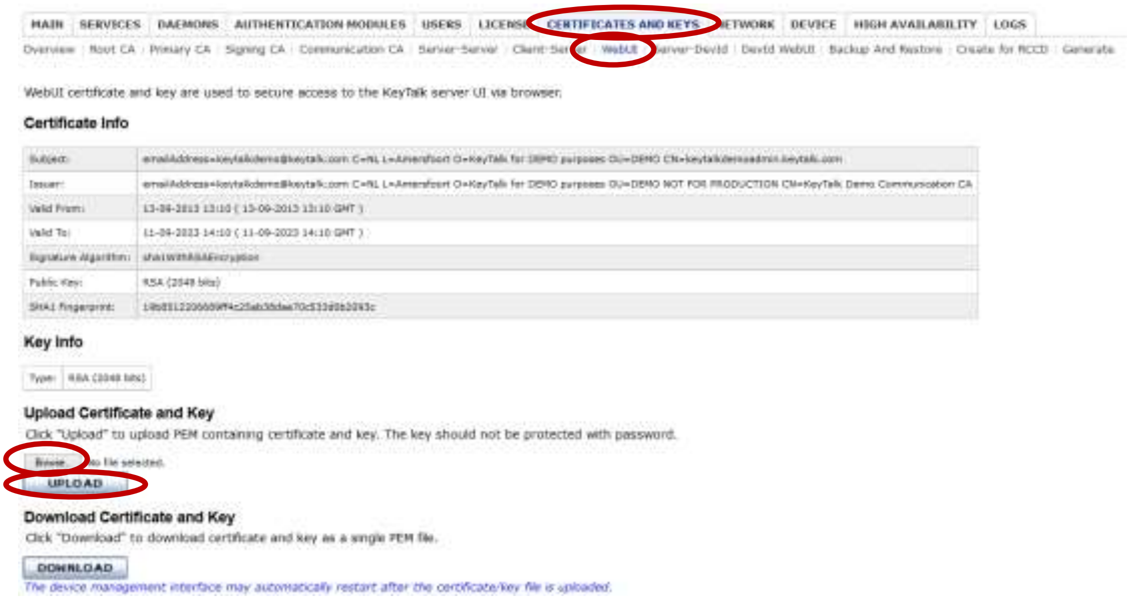
To avoid this warning you must install a certificate from a trusted party such as VeriSign, GoDaddy, GlobalSign, Cybertrust, or from your own KeyTalk Certificate Authority. See following section for details.

8.1. Replacing Admin GUI SSL-certificate

By default a self-signed SSL certificate is used to access the appliance over https://10.1.1.1:3000

You should replace this SSL certificate with your own. A certificate can also be obtained from a well-known party such as VeriSign, GoDaddy, Globalsign and Cybertrust.

In the main menu, select "CERTIFICATES AND KEYS" and select "WebUI". Upload your own SSL certificate by clicking on "Browse…", selecting the SSL certificate and clicking on "UPLOAD".



WebUI certificate and key are used to secure access to the KeyTalk server UI via browser.

Certificate Info

Subject:	emailAddress=keytalkdemo@keytalk.com C=NL L=Amersfoort O=KeyTalk for DEMO purposes OU=DEMO CN=keytalkdemoadmin.keytalk.com
Issuer:	emailAddress=keytalkdemo@keytalk.com C=NL L=Amersfoort O=KeyTalk for DEMO purposes OU=DEMO NOT FOR PRODUCTION CN=KeyTalk Demo Communication CA
Valid From:	13-09-2013 13:10 (13-09-2013 13:10 GMT)
Valid To:	11-09-2023 14:10 (11-09-2023 14:10 GMT)
Signature Algorithm:	sha1WithRSAEncryption
Public Key:	RSA (2048 bits)
SHA1 fingerprint:	18b8812206669ff4c25ab38daa70c533d0b2093c

Key Info

Type:	RSA (2048 bits)

Upload Certificate and Key

Click "Upload" to upload PEM containing certificate and key. The key should not be protected with password.

No file selected.

Download Certificate and Key

Click "Download" to download certificate and key as a single PEM file.

The device management interface may automatically restart after the certificate/key file is uploaded.

Figure 21: Replacing the SSL-certificate

Make sure that the SSL certificate you wish to make use of, also contains the private key, and is in a PEM file format.

Select the file by pressing BROWSE and press UPLOAD to replace the existing SSL certificate.

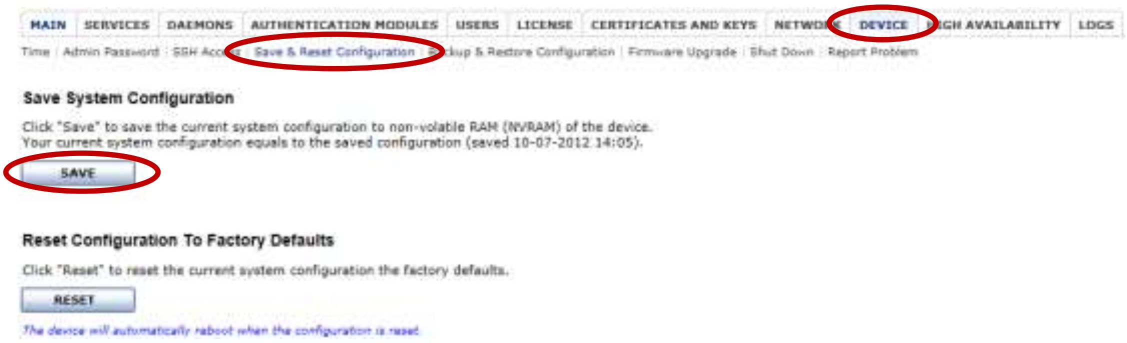
After a successful UPLOAD the device management subsystem will automatically restart to effectuate the new SSL certificate.

To make the changes permanent, please refer to section 8.2 ‘Saving changes & reboot’.

8.2. Saving changes & reboot

Changes made in the Admin GUI will be effective, as long as the KeyTalk appliance does not lose its electric power. In order to make changes permanent, the changes must be saved by the administrator.

SAVING: In the main menu select the “DEVICE” tab and select “Save & Reset Configuration”. Select “SAVE” to save the System Configuration.


MAIN | SERVICES | DAEMONS | AUTHENTICATION MODULES | USERS | LICENSE | CERTIFICATES AND KEYS | NETWORK | DEVICE | HIGH AVAILABILITY | LOGS
Time | Admin Password | SSH Access | Save & Reset Configuration | Backup & Restore Configuration | Firmware Upgrade | Shut Down | Report Problem
SAVE
RESET

Save System Configuration

Click "Save" to save the current system configuration to non-volatile RAM (NVRAM) of the device.
Your current system configuration equals to the saved configuration (saved 10-07-2012 14:05).

Reset Configuration To Factory Defaults

Click "Reset" to reset the current system configuration the factory defaults.

The device will automatically reboot when the configuration is reset.

Figure 22: Saving System configuration

REBOOT: In the main menu select the "DEVICE" tab and select "Shut Down". Select "REBOOT" to reboot the system.

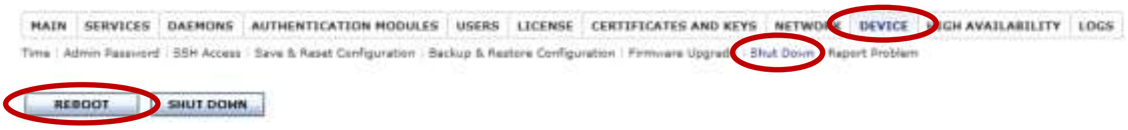

MAIN | SERVICES | DAEMONS | AUTHENTICATION MODULES | USERS | LICENSE | CERTIFICATES AND KEYS | NETWORK | DEVICE | HIGH AVAILABILITY | LOGS
Time | Admin Password | SSH Access | Save & Reset Configuration | Backup & Restore Configuration | Firmware Upgrade | Shut Down | Report Problem
REBOOT
SHUT DOWN

Figure 23: Rebooting the system

9. SSH

SSH is by default disabled on the KeyTalk appliance. Should there be a need to activate it, please contact your KeyTalk supplier for an updated KeyTalk license with activated SSH.

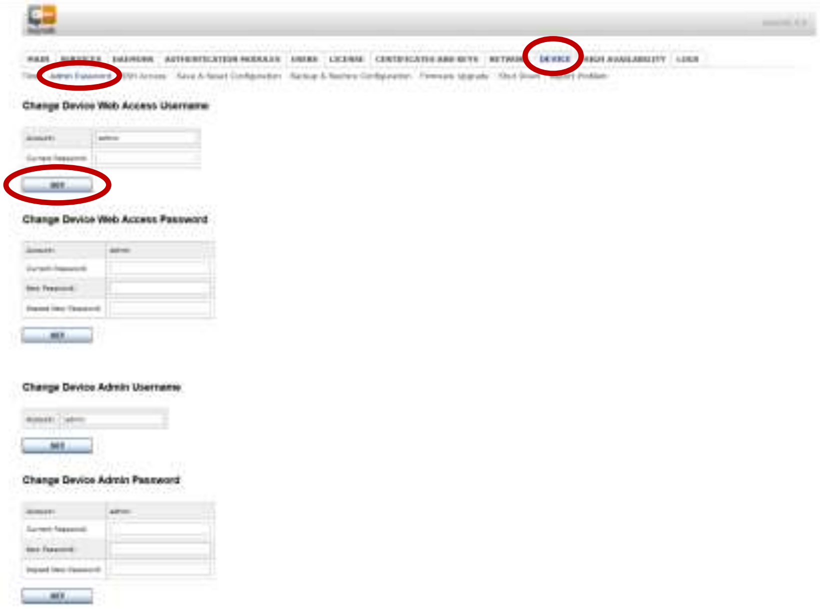
Those running VMware can access the device through their VMware software using the default:
User: admin
Pwd: change!
These may have been changed if the KeyTalk Admin has followed the guidelines under under section 10 of this manual

10. Changing KeyTalk passwords

The Graphical Administrator Interface can be used, when required, for administrator maintenance.

The Admin authentication credentials are by default set to:
Graphical Administrator Interface (Admin GUI):
User: admin
Password: change!

In order to change the Graphical Administrator Interface password, do the following:
In the upper menu select the ‘DEVICE’ tab and select ‘Admin Password’.



Change Device Web Access Username

Account:	admin
Current Password:	

SET

Change Device Web Access Password

Account:	admin
Current Password:	
New Password:	
Repeat New Password:	

SET

Change Device Admin Username

Account:	admin

SET

Change Device Admin Password

Account:	admin
Current Password:	
New Password:	
Repeat New Password:	

SET

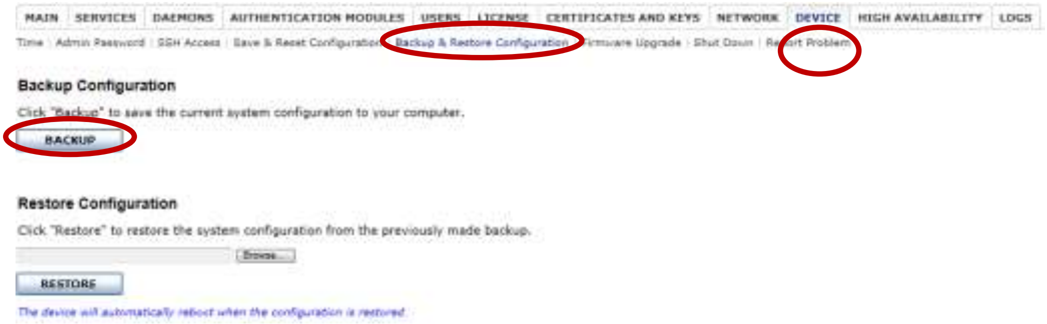
Figure 24: Changing Graphical Administrator Interface password

Enter both current and new password, and confirm the new password, in the Change Device Web Access Password fields. Press “OK” to activate the new password.
Note: *It is important to remember this password.*

The KeyTalk appliance also has a more powerful user, the device admin, for low level administrator maintenance. This user is not enabled by default. If required, contact your KeyTalk supplier or partner.

11. Backup and Restore

To make a full backup of your current system configuration to your computer, select “DEVICE” from the main menu, select “Backup & Restore Configuration” and select “BACKUP”.


MAIN
SERVICES
DAEMONS
AUTHENTICATION MODULES
USERS
LICENSE
CERTIFICATES AND KEYS
NETWORK
DEVICE
HIGH AVAILABILITY
LOGS
Time | Admin Password | SSH Access | Save & Reset Configuration | Backup & Restore Configuration | Firmware Upgrade | Shut Down | Report Problem
BACKUP
Browse...
RESTORE

Backup Configuration

Click "Backup" to save the current system configuration to your computer.

Restore Configuration

Click "Restore" to restore the system configuration from the previously made backup.

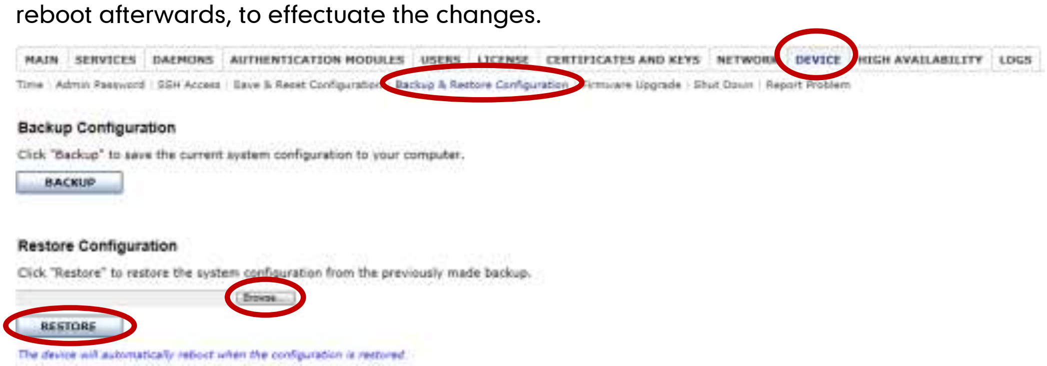
The device will automatically reboot when the configuration is restored.

Figure 25: Making a backup of the system configuration

Save the backup file “keytalk.config.dat” in a location of your choice.

To restore your backup of your system configuration, select “DEVICE” from the main menu, select “Backup & Restore Configuration” and select “Browse” under ‘Restore Configuration’.

Select your “keytalk.config.dat” backup file, and select “RESTORE”. The KeyTalk appliance will reboot afterwards, to effectuate the changes.


MAIN
SERVICES
DAEMONS
AUTHENTICATION MODULES
USERS
LICENSE
CERTIFICATES AND KEYS
NETWORK
DEVICE
HIGH AVAILABILITY
LOGS
Time | Admin Password | SSH Access | Save & Reset Configuration | Backup & Restore Configuration | Firmware Upgrade | Shut Down | Report Problem
BACKUP
Browse...
RESTORE

Backup Configuration

Click "Backup" to save the current system configuration to your computer.

Restore Configuration

Click "Restore" to restore the system configuration from the previously made backup.

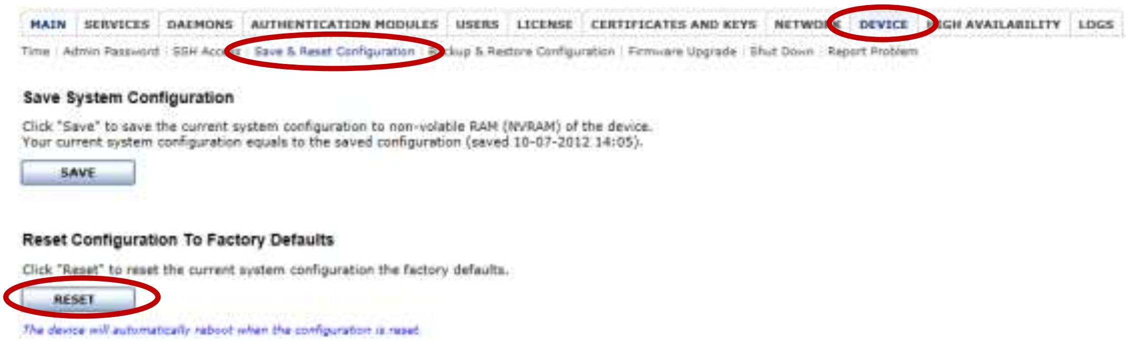
The device will automatically reboot when the configuration is restored.

Figure 26: Restoring the system configuration backup file

12. Factory Reset

Should you ever want to reset the KeyTalk appliance to its original factory settings, the steps described below must be followed.

Select from the main menu the “DEVICE” tab and select “Save & Reset Configuration”.
Select “RESET” to restore default factory configuration settings.



Save System Configuration

Click "Save" to save the current system configuration to non-volatile RAM (NVRAM) of the device.
Your current system configuration equals to the saved configuration (saved 10-07-2012 14:05).

Reset Configuration To Factory Defaults

Click "Reset" to reset the current system configuration the factory defaults.

The device will automatically reboot when the configuration is reset

Figure 27: Resetting the Factory Defaults

Note: *When resetting to the default factory configuration settings, this will also affect your set IP addresses!! In case your KeyTalk device is off premise, remote communication with the device will be impossible after a factory reset.*

13. Firmware upgrade

KeyTalk BV releases periodically new firmware for the KeyTalk appliance.

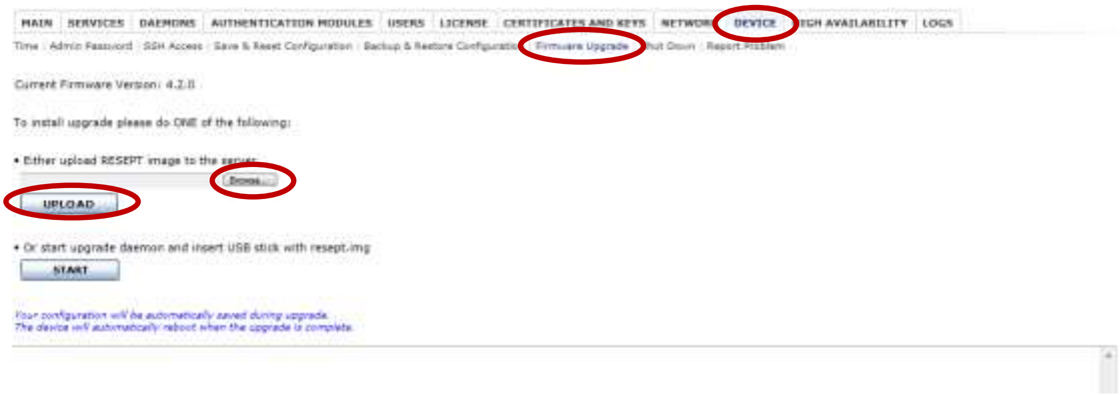
New firmware can fix bugs as well as add new functionality.

Upgrading requires you to go from one version to the next (i.e. 4.2 to 4.2.1 or to 4.3) in full sequential order. Skipping a firmware version in between will be detected by KeyTalk and result in an aborted upgrade and KeyTalk going back to its last persistent state.

Upgrading the KeyTalk firmware can be done in two different ways:

1. For remote upgrading, you can upload the upgrade-file via the administrator graphical interface (Admin GUI).

   Within the KeyTalk Admin GUI, go to "DEVICE", select "Firmware Upgrade", click on 'Browse' to select the upgrade-file and click on "UPLOAD" to start the upgrade process.



Current Firmware Version: 4.2.0

To install upgrade please do ONE of the following:

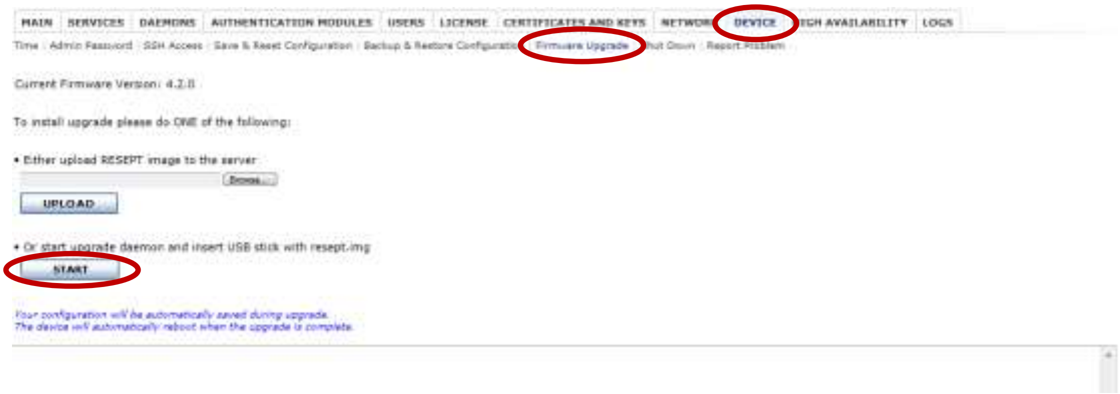
- Either upload RESEPT image to the server
- Or start upgrade daemon and insert USB stick with resept.img

Your configuration will be automatically saved during upgrade.
The device will automatically reboot when the upgrade is complete.

Figure 28: Firmware upgrade - remote

2. If you have physical access to the appliance, you can use a USB-stick for the upgrade.

   Within the KeyTalk Admin GUI, go to "DEVICE", select "Firmware Upgrade", insert the USB stick with the upgrade-files on it into one of the USB ports 'L' or 'M', the LCD menu will be activated. Click on "START" to upgrade. The system will HALT after an upgrade, requiring an additional reboot.



Current Firmware Version: 4.2.8

To install upgrade please do ONE of the following:

- Either upload RESEPT image to the server
- Or start upgrade daemon and insert USB stick with resept.img

Your configuration will be automatically saved during upgrade.
The device will automatically reboot when the upgrade is complete.

Figure 29: Firmware upgrade – on premise

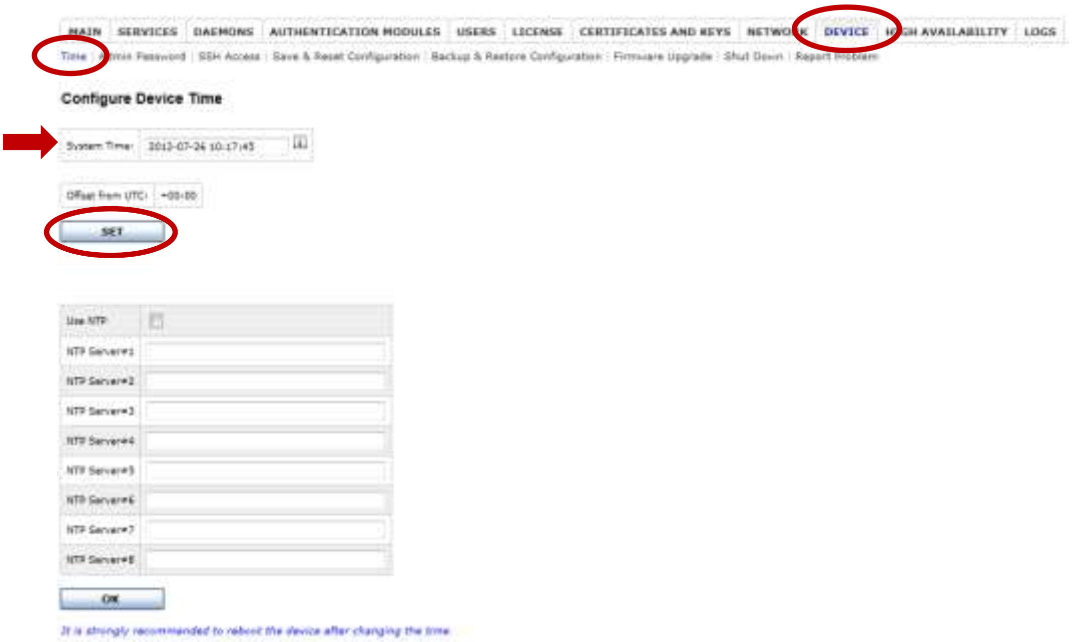
As a result the upgrade will start. The progress of the upgrade will be shown in the Admin GUI.

On successful upgrade, the appliance will automatically REBOOT to apply the new firmware while preserving the latest persistent configuration.

14. Date/time & NTP settings

To set the applicable **date/time**, go to the tab “DEVICE” and select “Time”.

Enter the current date and time in UTC (!), and select “SET”.


MAIN | SERVICES | DAEMONS | AUTHENTICATION MODULES | USERS | LICENSE | CERTIFICATES AND KEYS | NETWORK | DEVICE | HIGH AVAILABILITY | LOGS
Time | Admin Password | SSH Access | Save & Reset Configuration | Backup & Restore Configuration | Firmware Upgrade | Shut Down | Report Problem
SET
OK

Configure Device Time

System Time: 2013-07-26 10:17:45

Offset from UTC: +00:00

Use NTP ☐

NTP Server#1

NTP Server#2

NTP Server#3

NTP Server#4

NTP Server#5

NTP Server#6

NTP Server#7

NTP Server#8

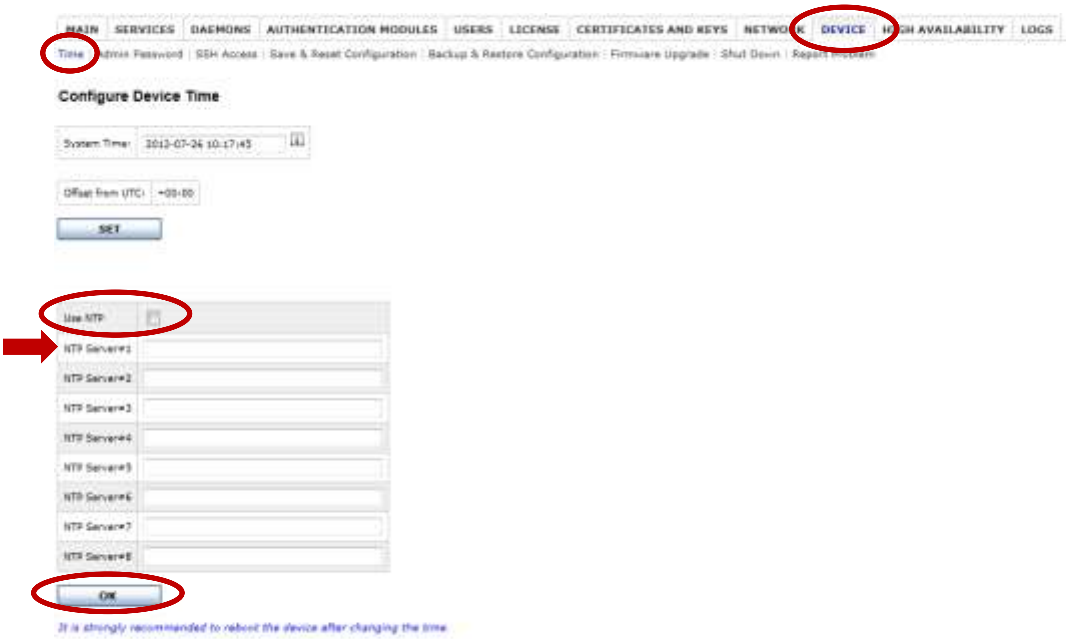
It is strongly recommended to reboot the device after changing the time

Figure 30: Setting the applicable date/time

Note: *The Netherlands is UTC+1 (during summertime UTC+2); CST = UTC-6 (during summertime UTC-5); EST = UCT-5 (during summertime UTC-4).*

It is highly recommended to set your applicable **NTP server(s)**.

When using NTP server(s) also check the ‘Use NTP’ box. Confirm by selecting “OK”.



Configure Device Time

System Time: 2013-07-26 10:17:45

Offset from UTC: +00:00

Use NTP □

NTP Server#1
NTP Server#2
NTP Server#3
NTP Server#4
NTP Server#5
NTP Server#6
NTP Server#7
NTP Server#8

It is strongly recommended to reboot the device after changing the time

Figure 31: Set your applicable NTP server(s)

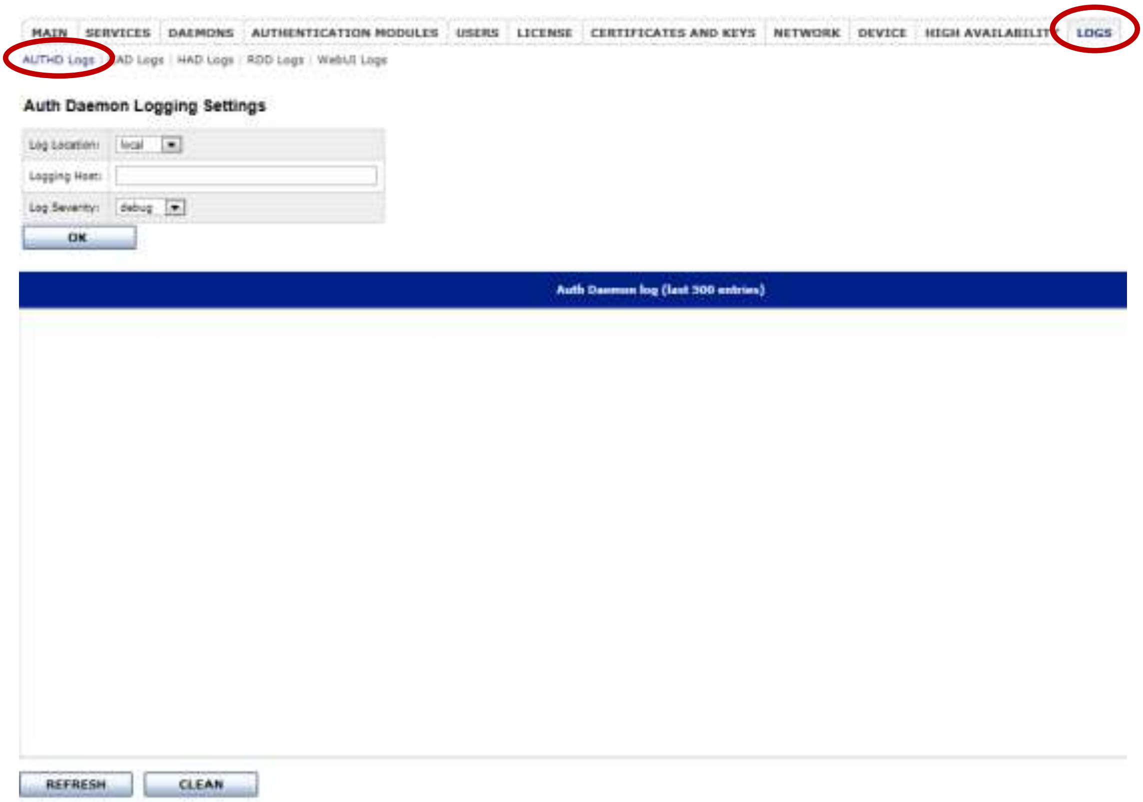
See section 5.8 ‘Step 8: DNS & NTP/Date Time customization’ for details on setting the time for DNS and NTP. There are two menu items to configure the time, but both function identically. One menu item is located in the ‘Network configuration’, the other in ‘Device configuration’. Both direct you to the same function.

15. Log files

The log files of the four main Daemons and the Web UI can be accessed from the tab "LOGS" in the upper menu:

- AUTHD Logs – Authentication daemon logs
- CAD Logs – Certificate Authority daemon logs
- HAD Logs – High Availability daemon logs
- RDD Logs – RESEPT Dispatcher daemon logs (KeyTalk's previous name was RESEPT)
- WebUI Logs – Web interface logs

For example, from the main menu, select the "LOGS" tab and select "AUTHD Logs".



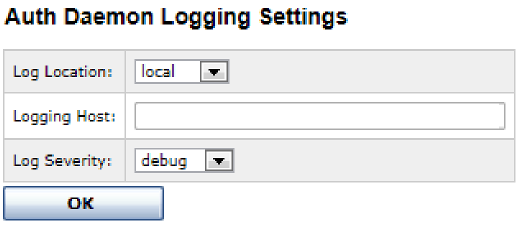
Auth Daemon Logging Settings

Log Location:	local
Logging Host:	
Log Severity:	debug

Figure 32: Authentication daemon logs

15.1. Daemon logging settings

Each Daemon and the Web UI have their own log destination that can be configured individually.



Auth Daemon Logging Settings

Log Location:	local
Logging Host:	
Log Severity:	debug

Figure 33: Daemon logging settings, e.g. for the authentication daemon log

Log Location allows the Admin to choose between local logging (default) and remote logging.

When local logging is chosen, the appropriate Daemon's log file will be stored on the local KeyTalk appliance until it reaches a 250k size. After that the local log file rotates to a fresh log file.

Choosing remote logging requires setting a host. Remote logging will allow for a continuous log file on your syslog-server.

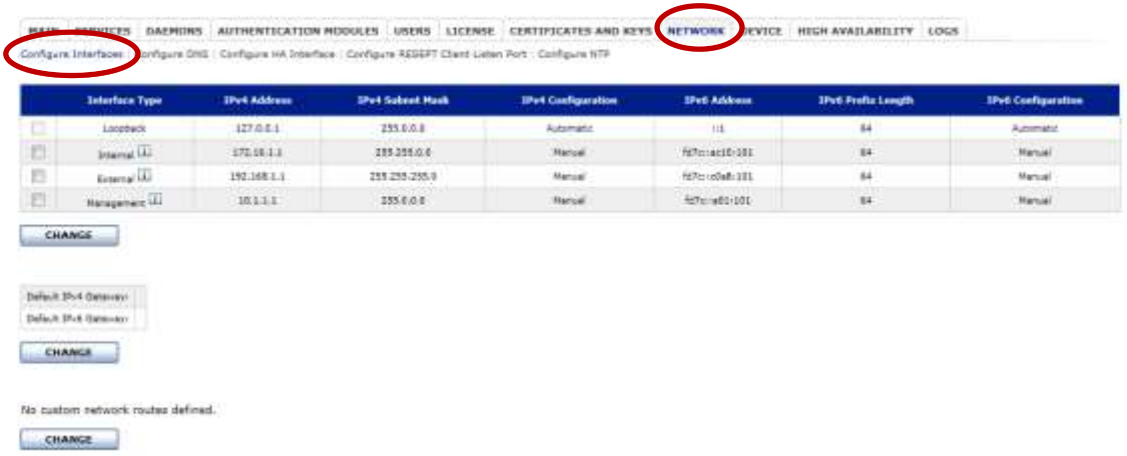
Log Severity allows from minimal logging using the "emerg" (= emergency), to the standard log level of "warning", up to the most comprehensive log file under the "*" or "debug" setting.

16. Network settings

16.1. Configure interfaces

To configure the network, network administration knowledge is required.

The KeyTalk appliance makes use of four interfaces. These can be configured by selecting from the main menu “NETWORK”, followed by selecting “Configure Interfaces”.



	Interface Type	IPv4 Address	IPv4 Subnet Mask	IPv4 Configuration	IPv6 Address	IPv6 Prefix Length	IPv6 Configuration
□	Loopback	127.0.0.1	255.0.0.0	Automatic	::1	64	Automatic
□	Internal ⓘ	172.16.1.1	255.255.0.0	Manual	fd7c::ac10:101	64	Manual
□	External ⓘ	192.168.1.1	255.255.255.0	Manual	fd7c::c0a8:101	64	Manual
□	Management ⓘ	10.1.1.1	255.0.0.0	Manual	fd7c::a01:101	64	Manual

Default IPv4 Gateway:
Default IPv6 Gateway:

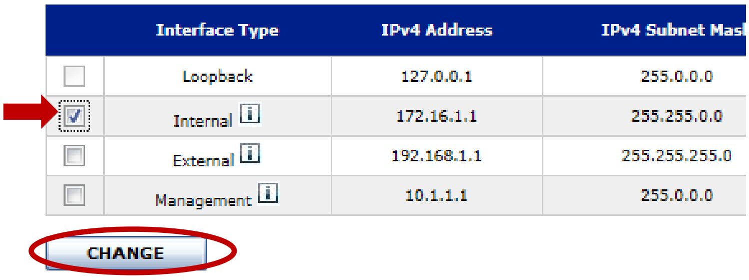
No custom network routes defined.

Figure 34: Configuring interfaces

Interface Types

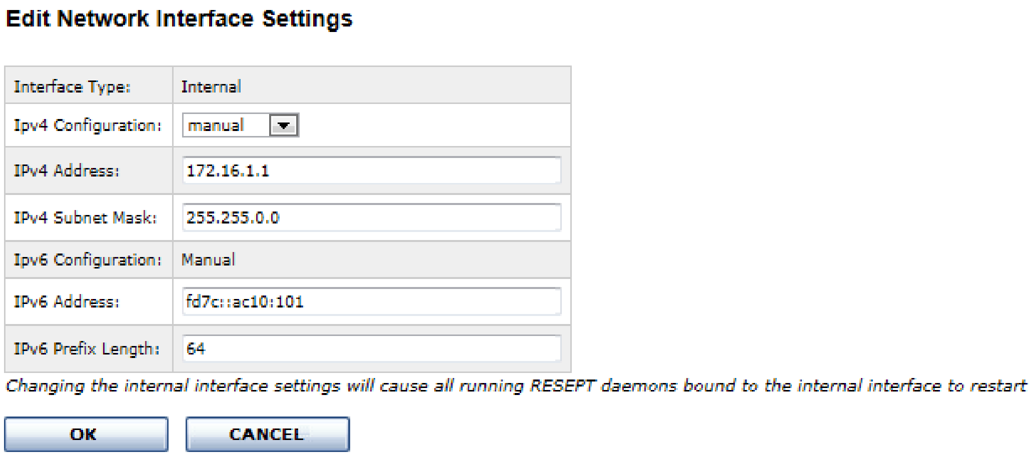
Loopback:	cannot be configured from the Admin GUI
Internal:	corresponds to NIC “O”, see Section 3 ‘Back Panel Components’
External:	corresponds to NIC “Q”, see Section 3 ‘Back Panel Components’
Management:	corresponds to NIC “P”, see Section 3 ‘Back Panel Components’

To configure a specific interface, select the appropriate box and click on “CHANGE”.



	Interface Type	IPv4 Address	IPv4 Subnet Masl
□	Loopback	127.0.0.1	255.0.0.0
☑	Internal ⓘ	172.16.1.1	255.255.0.0
□	External ⓘ	192.168.1.1	255.255.255.0
□	Management ⓘ	10.1.1.1	255.0.0.0

Figure 35: Changing the Internal Interface type



Edit Network Interface Settings

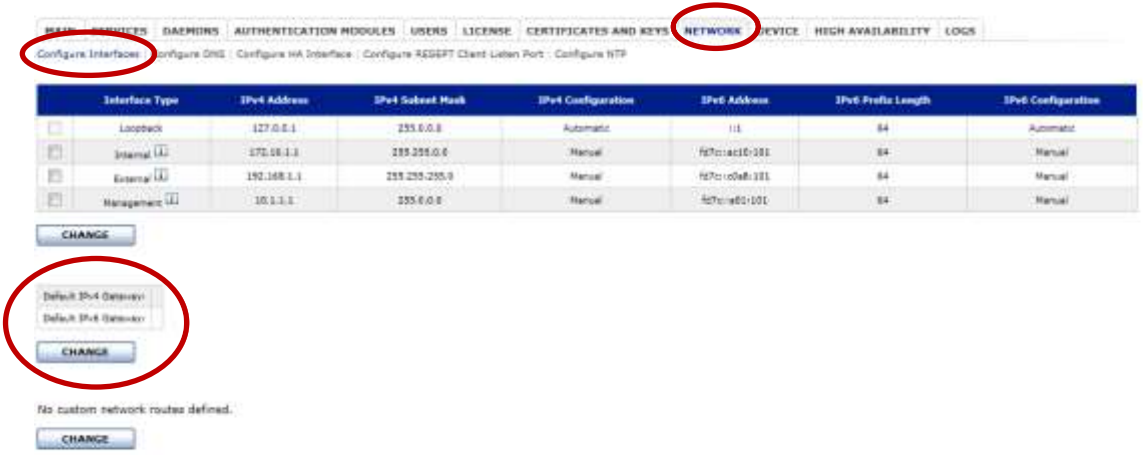
Interface Type:	Internal
Ipv4 Configuration:	manual
IPv4 Address:	172.16.1.1
IPv4 Subnet Mask:	255.255.0.0
Ipv6 Configuration:	Manual
IPv6 Address:	fd7c::ac10:101
IPv6 Prefix Length:	64

Changing the internal interface settings will cause all running RESEPT daemons bound to the internal interface to restart

Figure 36: Edit Network interface settings

Configure the items you wish to change and select “OK” to save these changes.

To change the KeyTalk appliance default gateway, select from the main menu “NETWORK”, select “Configure Interfaces” and select “CHANGE”.



MAIN | SERVICES | DAEMONS | AUTHENTICATION MODULES | USERS | LICENSE | CERTIFICATES AND KEYS | NETWORK | DEVICE | HIGH AVAILABILITY | LOGS
Configure Interfaces | Configure DNS | Configure HA Interface | Configure RESEPT Client Listen Port | Configure NTP

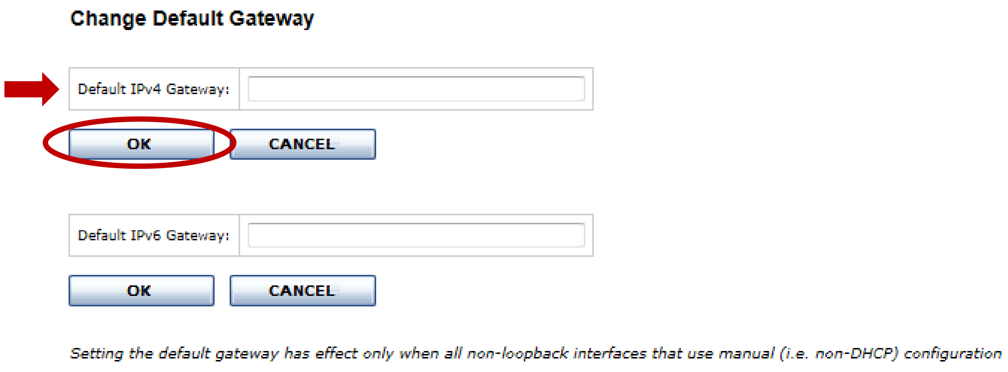
	Interface Type	IPv4 Address	IPv4 Subnet Mask	IPv4 Configuration	IPv6 Address	IPv6 Prefix Length	IPv6 Configuration
□	Loopback	127.0.0.1	255.0.0.0	Automatic	::1	64	Automatic
□	Internal	172.16.1.1	255.255.0.0	Manual	fd7c::ac10:101	64	Manual
□	External	192.168.1.1	255.255.255.0	Manual	fd7c::c0a8:101	64	Manual
□	Management	10.1.1.1	255.0.0.0	Manual	fd7c::a01:101	64	Manual

Default IPv4 Gateway:
Default IPv6 Gateway:

No custom network routes defined.

Figure 37: Changing default Gateway

On the screen that opens, configure the default gateway IP and select “OK”.



Change Default Gateway

Default IPv4 Gateway:

Default IPv6 Gateway:

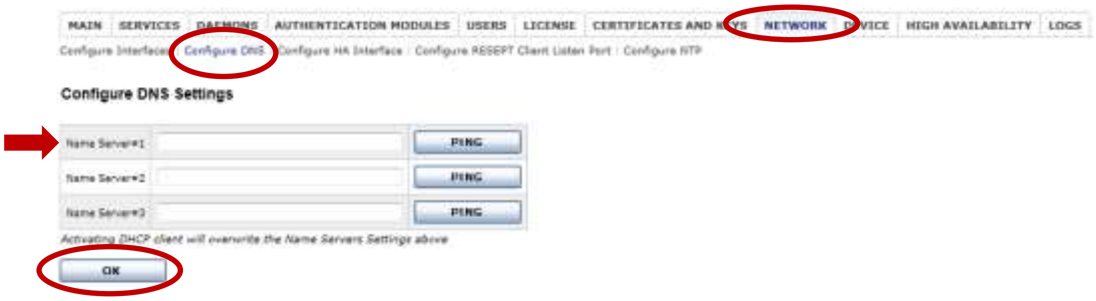
Setting the default gateway has effect only when all non-loopback interfaces that use manual (i.e. non-DHCP) configuration

Figure 38: Changing the default gateway

Note: *Optionally you can set a gateway for each NIC separately.*

16.2. Configure DNS

To set your applicable DNS, from the upper menu select "NETWORK" and select "Configure DNS".



Configure DNS Settings

Name Server#1

Name Server#2

Name Server#3

Activating DHCP client will overwrite the Name Servers Settings above

Figure 39: Configuring DNS

Enter the IP addresses of your DNS and select 'OK'.

Note: *Do not enter host name, but IP addresses.*

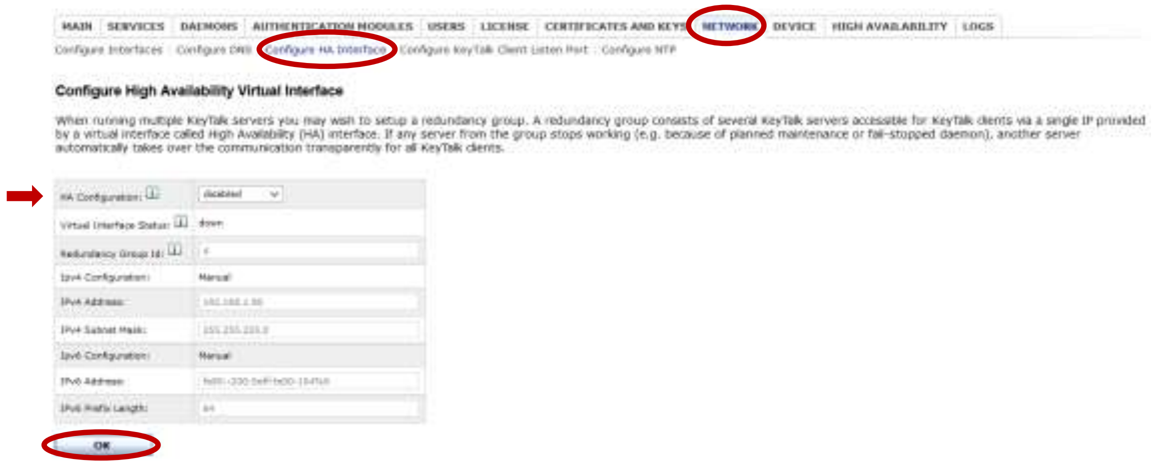
16.3. Configure High Availability Virtual Interface

When running multiple KeyTalk servers you may wish to combine them in a redundancy group.

One logical KeyTalk server maps of one or more physical KeyTalk appliances (servers) sharing the same redundancy group ID. From the KeyTalk Client perspective it behaves as one server with one IP address. This IP address is provided by a virtual interface called High Availability (HA) interface.

When any server from the group stops working, another server from the same group automatically takes over the communication transparently for all KeyTalk clients
High Availability is not a substitute for load balancing. The current limitation of the High Availability for the KeyTalk appliance is that it is bound to one network ip-range.

To configure the High Availability, from the main menu select "NETWORK", then select "Configure HA Interface".



Configure High Availability Virtual Interface

When running multiple KeyTalk servers you may wish to setup a redundancy group. A redundancy group consists of several KeyTalk servers accessible for KeyTalk clients via a single IP provided by a virtual interface called High Availability (HA) interface. If any server from the group stops working (e.g. because of planned maintenance or fail-stopped daemon), another server automatically takes over the communication transparently for all KeyTalk clients.

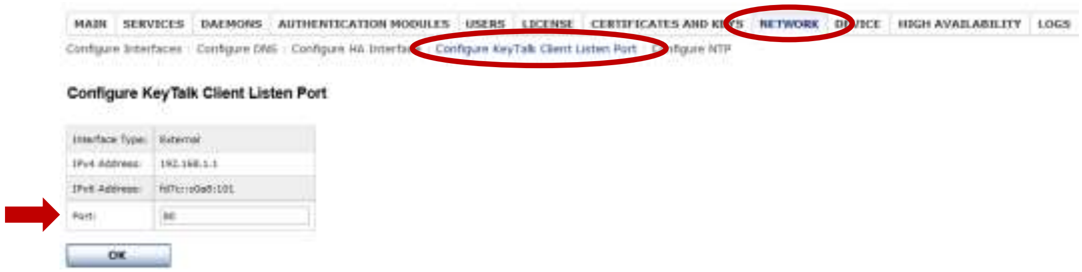
HA Configuration:	disabled
Virtual Interface Status:	down
Redundancy Group Id:	4
Ipv4 Configuration:	Manual
IPv4 Address:	192.168.1.50
IPv4 Subnet Mask:	255.255.255.0
Ipv6 Configuration:	Manual
IPv6 Address:	fe80::230:5eff:fe00:154%8
IPv6 Prefix Length:	64

Figure 40: Configuring the High Availability Virtual Interface

Make the appropriate configuration changes and select "OK".

16.4. Configure KeyTalk client listening port

It is very unlikely that you will have to change the port number on which the KeyTalk appliance listens to the KeyTalk Client; as the default 80 port will pass most firewalls. If you would like to change the port, select from the main menu "NETWORK", and select "Configure RESEPT Client Listen Port".



Configure KeyTalk Client Listen Port

Interface Type:	External
IPv4 Address:	192.168.1.1
IPv6 Address:	fd7c::c0a8:101
Port:	80

Figure 41: Configuring the KeyTalk client listening port

Change the port number and select "OK" to save the change. Additionally you must use KeyTalk Configuration Tool to change port number on your KeyTalk client, but preferably update it in the RCCD file by creating and singing a new one using KeyTalk's signingportal

17. Configuring daemons

In Unix and other multitasking computer operating systems, a daemon is a computer program that runs as a background process, rather than being under the direct control of an interactive user (*source: Wikipedia.org*).

The following daemons are important for proper functioning of the KeyTalk appliances:

- **AUTHD – Authentication daemon**
  Responsible for the user authentication process. It will connect to the applicable authentication database.
- **CAD– Certificate Authority daemon**
  The actual creator of the certificate. It will be invoked after successful authentication.
- **HAD– High Availability daemon**
  Responsible for the high availability functionality of the KeyTalk solution.
- **RDD – RESEPT Distribution daemon**
  All KeyTalk client traffic goes through RDD. This daemon will validate user input and will take responsibility for the distribution of the workflow to the other daemons.

Two daemons, CAD and HAD, can be configured in the tab "DAEMONS".

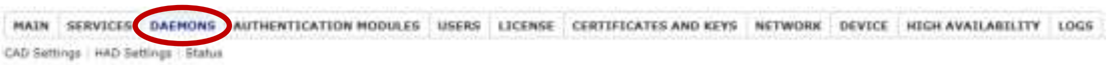
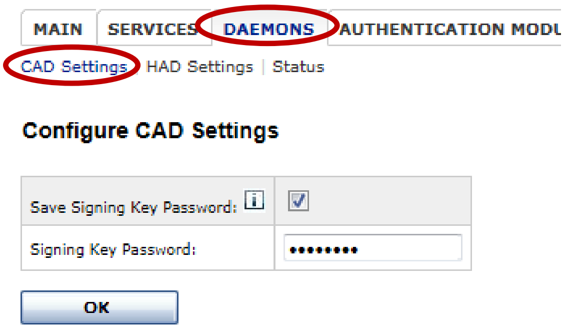


Figure 42: Configuring daemons

In the next sub-sections it is described how these two daemons can be configured.

17.1. Certificate Authority daemon (CAD) settings

To configure the Certificate Authority daemon, select "CAD Settings" in the "DAEMON" tab.



Configure CAD Settings

Save Signing Key Password:	☑
Signing Key Password:	••••••••

OK

Figure 43: Configuring the CAD Settings

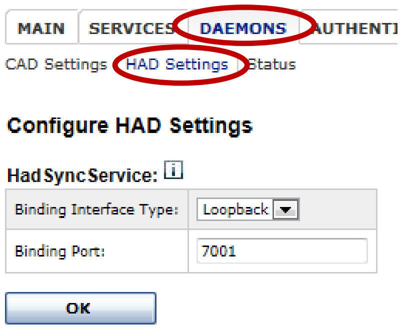
The CAD is responsible for the creation of the user certificates and keys.

When a password is present on your CAD Signing Key you may wish to store it for REBOOT purposes. The default password on the KeyTalk DEMO is blank.

Select “OK” to save.

17.2. High Availability daemon settings

To configure the High Availability daemon, select “HAD Settings” in the “DAEMON” tab.



Configure HAD Settings

Had Sync Service:

Binding Interface Type:	Loopback
Binding Port:	7001

Figure 44: Configuring the HAD Settings

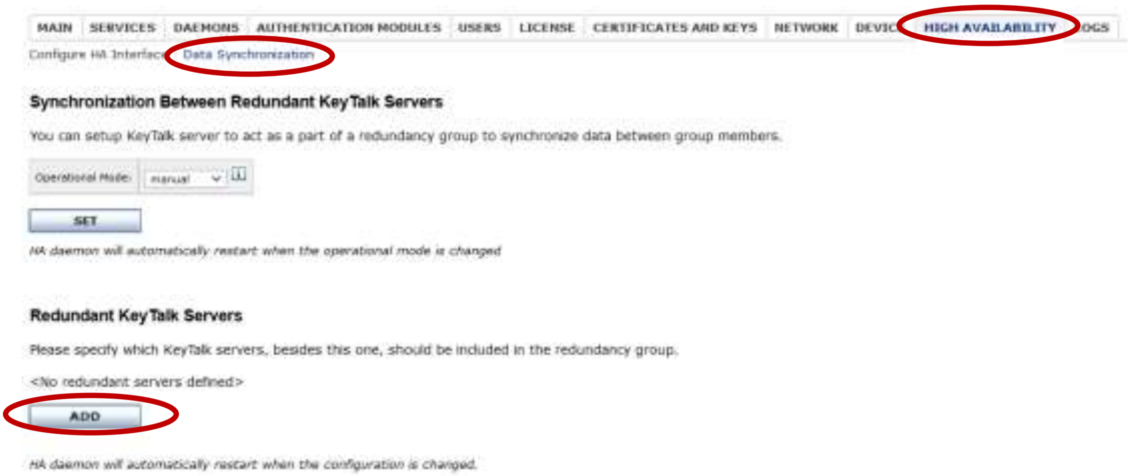
The HAD is responsible for discovery and synchronization between the other physical KeyTalk appliances.

Select the Binding Interface Type:

- Loopback
  (See Section 16.1 ´Configure interfaces´ for the description of this interface type)
- Internal
  (See Section 16.1 ´Configure interfaces´ for the description of this interface type)

Select “OK” to save the new settings.

Note: *High Availability daemons from other KeyTalk chains will need to be made known to the KeyTalk in order for HAD to work properly and loopback will need to be changed to internal when you wish to activate the HA.*



Synchronization Between Redundant KeyTalk Servers

You can setup KeyTalk server to act as a part of a redundancy group to synchronize data between group members.

Operational Mode: manual

HA daemon will automatically restart when the operational mode is changed

Redundant KeyTalk Servers

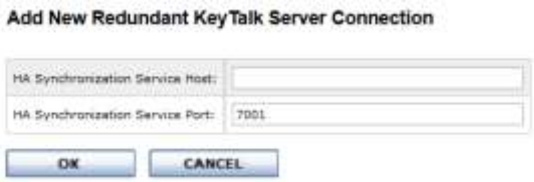
Please specify which KeyTalk servers, besides this one, should be included in the redundancy group.

<No redundant servers defined>

HA daemon will automatically restart when the configuration is changed.

Figure 45: HADs from other KeyTalk servers need to be made known

Select “ADD” to add a new KeyTalk appliance.



Add New Redundant KeyTalk Server Connection

HA Synchronization Service Host:

HA Synchronization Service Port: 7001

Figure 46: Add new HAD connection

Enter the HadSyncService Host and Port.

Select “OK” to save the settings.

17.2.1. High Availability in depth

The KeyTalk High Availability allows for a multiple physical KeyTalk servers to be made available in case of redundancy requirements.

A redundancy group consists of several KeyTalk servers accessible for KeyTalk clients via a single IP provided by a virtual interface called High Availability (HA) interface. If any server from the group stops working (e.g. because of planned maintenance or fail-stopped daemon), another server automatically takes over the communication transparently for all KeyTalk clients. Only one server from a group can route traffic from KeyTalk clients. This server is called “master” and the rest servers are called “slave”. Master-slave election occurs automatically and is transparent for KeyTalk clients.

***Note:** High Availability functionality is not a replacement for load balancing functionality.*

An example of a HA implementation could be:

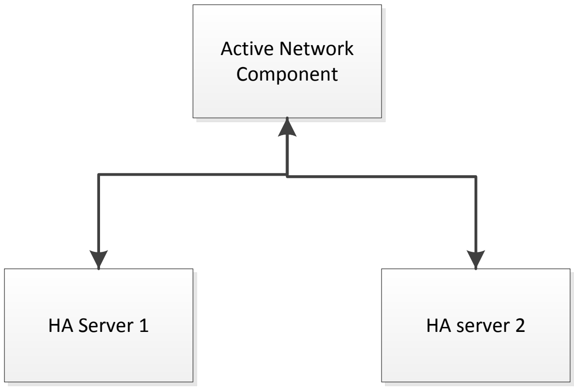


Figure 47: Example HA implementation

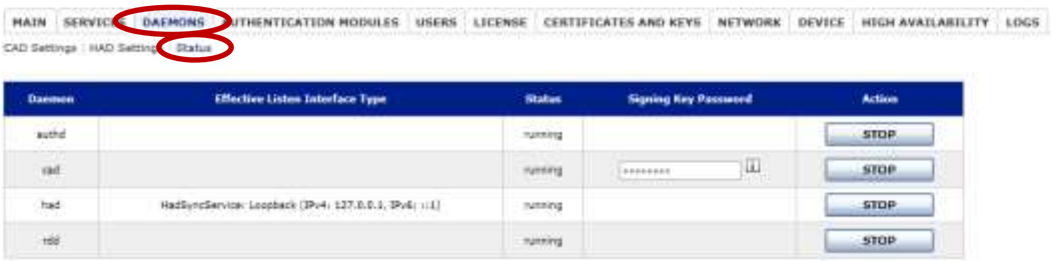
Each server in HA redundant group must be configured with the static information (ie IP numbers). All dynamic information (certificate serials, users etc.) is automatically synchronized, as soon as the chains have been configured to be aware of each other.

To ease configuration, it is a good starting point to always configure one single KeyTalk appliance, and make a backup of its configuration.

Note: *A configured copy might cause conflicting IP's, so configure with care.*

17.3. Stop/start daemons & status

The main daemons can be stopped / started from the status panel.



Daemon	Effective Listen Interface Type	Status	Signing Key Password	Action
authd		running		STOP
cad		running	••••••••	STOP
had	HadSyncService: Loopback (IPv4: 127.0.0.1, IPv6: ::1)	running		STOP
rdd		running		STOP

Figure 48: Stop/start daemons & status

When the CAD is started the Signing Key password may need to be entered when the password has been implemented.

To alleviate work for the Admin, it is possible to store the password. This can have security implications, but it has been made available to fit the company's security policy.

How to store the CAD signing key password is described in section 17.1 'Certificate Authority daemon (CAD) settings'.

18. Services

A service is a group of users that follow the same authentication method and default certificate time-to-live. Usually this group of users belongs to the same department/organization/company or use the same type of device.

Services define default values you wish to make available in the client X.509v3 certificates created, distributed and installed by KeyTalk. An example value for the organization attribute is ‘O’ = ‘Example.com’.

Additionally attributes in the certificate can be mapped to Active Directory attribute fields.

Multiple services can be configured, allowing you to set up a multitude of services on a single KeyTalk instance.

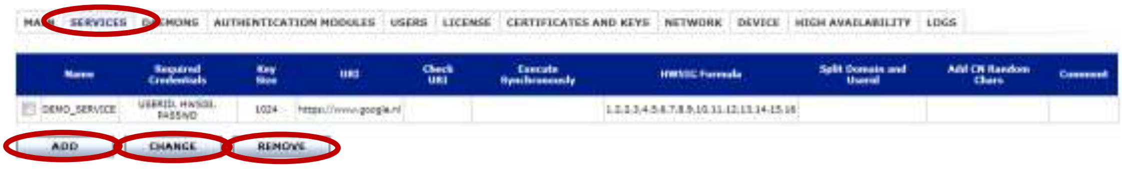
18.1. Creating/modifying a service

To manage services, select from the main menu “SERVICES”.

An overview of the existing services is displayed. In this overview, you will find a summary of the services’ settings and applicable comments.

The following options are available for Services:

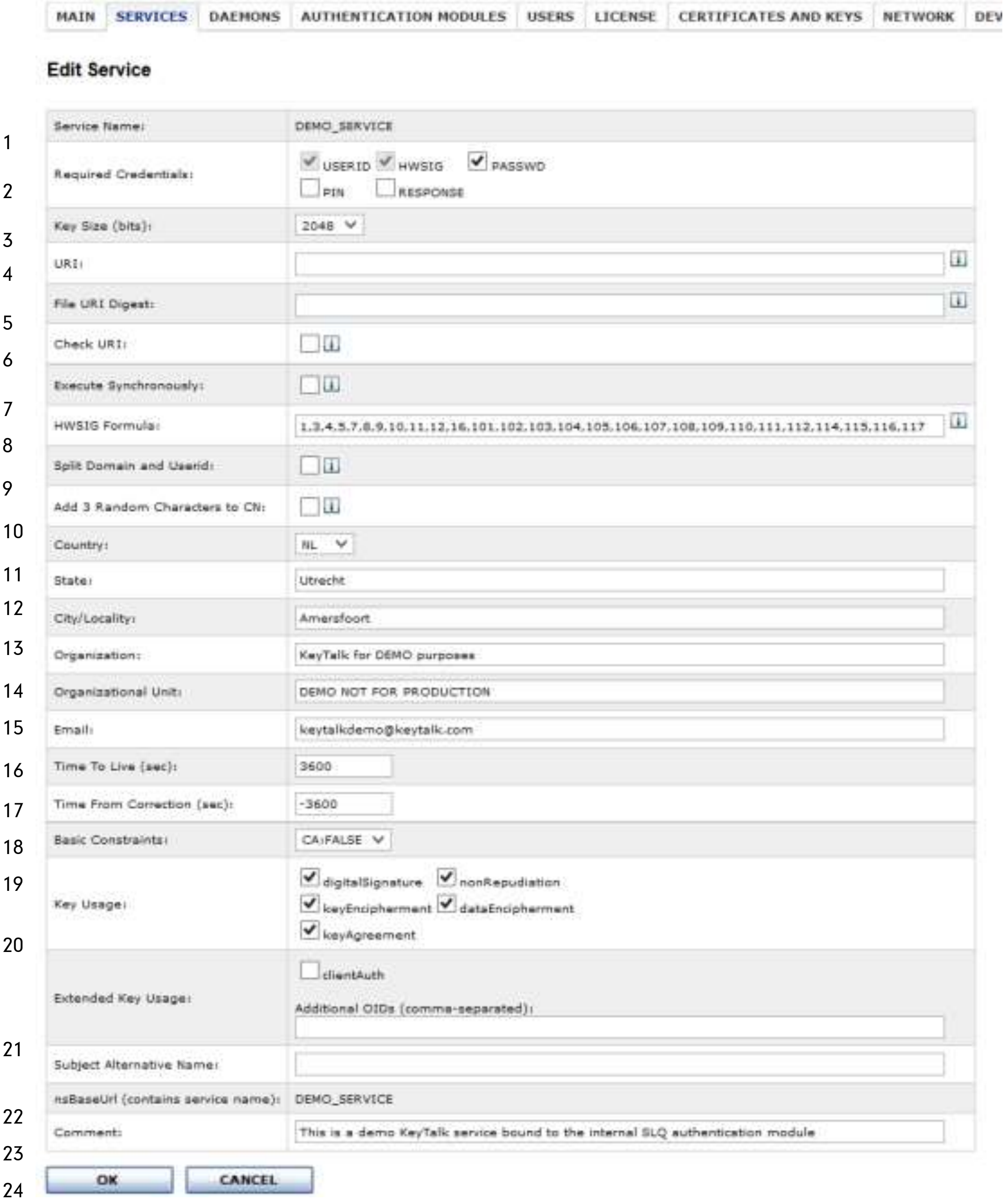
- Add
  Click on “ADD”
- Modify
  Select the existing service and click on “CHANGE”
- Delete
  Select the existing service and click on “REMOVE”



	Name	Required Credentials	Key Size	URI	Check URI	Execute Synchronously	HWSIG Formula	Split Domain and Userid	Add CN Random Chars	Comment
□	DEMO_SERVICE	USERID, HWSIG, PASSWD	1024	https://www.google.nl			1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16			

Figure 49: Adding/modifying/deleting a service

The following pages describe all the fields of the service.



Edit Service

1	Service Name:	DEMO_SERVICE
2	Required Credentials:	☑ USERID ☑ HWSIG ☑ PASSWD □ PIN □ RESPONSE
3	Key Size (bits):	2048
4	URI:	
5	File URI Digest:	
6	Check URI:	□
7	Execute Synchronously:	□
8	HWSIG Formula:	1,3,4,5,7,8,9,10,11,12,16,101,102,103,104,105,106,107,108,109,110,111,112,114,115,116,117
9	Split Domain and Userid:	□
10	Add 3 Random Characters to CN:	□
11	Country:	NL
12	State:	Utrecht
13	City/Locality:	Amersfoort
14	Organization:	KeyTalk for DEMO purposes
15	Organizational Unit:	DEMO NOT FOR PRODUCTION
16	Email:	keytalkdemo@keytalk.com
17	Time To Live (sec):	3600
18	Time From Correction (sec):	-3600
19	Basic Constraints:	CA:FALSE
20	Key Usage:	☑ digitalSignature ☑ nonRepudiation ☑ keyEncipherment ☑ dataEncipherment ☑ keyAgreement
21	Extended Key Usage:	□ clientAuth Additional OIDs (comma-separated):
22	Subject Alternative Name:	
23	nsBaseUrl (contains service name):	DEMO_SERVICE
24	Comment:	This is a demo KeyTalk service bound to the internal SLQ authentication module

Figure 50: Edit a service

1	Service Name	The name assigned to the Service.
2	Required Credentials	Select what authentication process and credentials are required These credentials will be requested from the KeyTalk Client configured with the given service. UserID and HwSig (Hardware signature) are always on and will be sent from the client to the server; PASSWD (password), PIN, and (Challenge)RESPONSE are all optional.
3	Key Size (bits)	Use the dropdown list to select the preferred RSA key length: 512, 1024, 2048 or 4096 bits. Note that the key size should not exceed the chosen key length of the CAD daemon signing certificate. If in doubt about the correct key size, consult your KeyTalk supplier or partner.
4	URI	This is the URI pushed from the KeyTalk appliance to the KeyTalk Client using the specific service. Leave empty when nothing needs to be invoked. When using a URL it can be used to trigger the KeyTalk client when an appropriately supported browser goes to the specific base URL. For example: https://webdemo.reseptdemo.com. Alternatively when the KeyTalk client has obtained the certificate, the client will start the specified URI. Instead of a URL the URI can also contain a reference to a local file or program. For example file://yourfilelocation/yourfilename. ***Note:*** *environment variables are respected.* Starting a program filename can also be done using parameters. Note that " " must be used when spaces are included in a path or using space separated parameters. ***Note:*** *Be careful not to use http:// addresses as these are not secure.*
5	File URI Digest	Optional field containing the SHA-256 of "file://" URI
6	Check URI	Tick to force a verification of the URI. When a URL is used, the IP needs to match both server and client side. When an executable is started the SHA-256 will be calculated and verified. For all the other URI schemes, including empty URI, no verification is performed.
7	Execute Synchronously	When the URI is an executable, this option allows you to set the client to run synchronously (KeyTalk client will run until the executable finishes) when selected or asynchronously when not selected.

8	HwSIG Formula	The HwSig formula specifies the list of hardware components on the user's device used for calculation of Hardware Signature (HwSig). The formula is comma separated and can contain the HwSig component number references in any order and as often as you like. Do note that the order and repetition of component numbers matters. For example: 0,1,2,3,4,5 or 0,0,0,6,7,3,3,8,9,14,11 For more information on the HwSig, please refer to Section 18.2 'Hardware Signature'.
9	Split Domain and Userid	Indicates whether an authentication module should split a fully-qualified userid supplied as domain\userid on two separate credentials. Currently only LDAP authentication module supports domain credentials.
10	Add 3 Random Characters to CN	When selected three random characters are added to the Common Name of the generated user certificate. This option is only needed for backward compatibility.
11	Country	The default value of the country code (ISO 3166 standard) as it should occur in the user certificate.
12	State	The default value of the state, county or province as it should occur in the user certificate.
13	City/Locality	The default value of the city/locality as it should occur in the user certificate.
14	Organization	The default value of the organization as it should occur in the user certificate.
15	Organizational Unit	The default value of the organizational unit as it should occur in the user certificate.
16	Email	The default value email address of the organization as it occurs in the user certificate.
17	Time To Live (sec)	The default amount of time, expressed in seconds, that a certificate is valid from the time it was issued.
18	Time For Correction (sec)	The default time correction factor, expressed in seconds, to correct problems when the Client system time is slightly off.
19	Basic Constraints	CA:FALSE = The generated certificate is a user certificate. CA:TRUE = The generated certificate is a CA certificate and is allowed to issue certificates (for advanced use only).
20	Key Usage	digitalSignature = *Allows for digital signing* nonrepudiation = *Qualifies a digital signature for non-repudiation* keyEncipherment = *Allows for encryption of keys* dataEncipherment = *Allows for encryption of data* keyAgreement = *Allows for SSL/key handshaking*

21	Extended Key Usage	Used for 802.1x EAP/TLS user certificate based authentication. Additional OIDs (comma-separated): Refer to http://www.openssl.org/docs/apps/x509v3_config.html#Extended_Key_Usage_ for more information.
22	Subject Alternative Name	The default value of the alternative subject name. For more values refer to: http://www.openssl.org/docs/apps/x509v3_config.html#Subject_Alternative_Name for more information.
23	nsBaseURL (contains service name)	Optional Netscape Base URL extension (see MSDN topic: http://msdn.microsoft.com/en-us/library/aa378149%28v=vs.85%29.aspx for more information.
24	Comment	Free text allowing for comments for Admin support purposes. This field will not be added to the certificate.

Note: *Key Usage fields should only be manipulated when you are familiar with their exact functionality and the impact they might have on application/server functionality.*
For more information refer to RSA-Labs (http://www.rsa.com/rsalabs/) and RFC 5280 (http://tools.ietf.org/html/rfc5280).

Note: *If not familiar with the exact functionality, it is advised to use the KeyTalk default values for the certificate attributes.*

18.2. Hardware Signature

KeyTalk can optionally determine the state of hardware of a user’s device, by calculating a hash over several components of the user’s computer hardware.

The components can be chosen from the list below, and are applied in the HwSig formula as described in section 18.1 ‘Creating/modifying a service’.

The following component IDs are supported on Windows devices:

0 Predefined value.

1 Primary HDD Serial. On Windows primary HDD is defined by minimal i for which \\.\PhysicalDrive<i> or \\.\Scsi<i> is accessible.

2 Primary NIC MAC-address. On Windows primary NIC is the NIC listed first in the "Network Connections" folder-> Advanced menu -> Advanced settings list.

3 HDDs Device Instance IDs. Only HDDS attached to IDE and SCSI are considered to avoid pluggable disks e.g. USB, PCI. Note SATA and eSATA, or PCMCIA will be used when available.

4 NICs Device Instance IDs. Only NICs attached to PCI are considered to avoid pluggable NICs e.g. USB.

5 IDE ATA/ATAPI controllers Device Instance IDs, excluding hot-pluggable one’s like e.g. PCMCIA.

6 USB Root Hubs Device Instance IDs.

7 Display Adapters Device Instance IDs.

8 Amount of physical memory.

9 CPUs device instance IDs.

10 Interrupt controller device instance ID.

11 System timer device instance ID.

12 DMA controller device instance ID.

13 System speaker device instance ID.

14 OS Product ID.

15 OS registered owner.

16 User Security Identifier.

17 BIOS serial number

iOS client codes:

101 Device name as set by user, e.g. "KeyTalk".

102 Operating System name e.g. "iPhone OS".

103 Model of the device e.g. "iPad".

104 Model of the device as a localized string.

105 Software defined UDID, real hardware UDID is deprecated by Apple. Example "e510de852117a695d04048e8e42".

106 Unique application ID, e.g. "com.keytalk.client".

107 Platform identification string, e.g. "iPad3,1".

108 Specific hardware model description, e.g. "J1AP".

109 Platform friendly name, derived from Platform - e.g. "iPad 3G".

110 CPU Frequency. For example 1000000000.

111 BUS Frequency. For example 250000000.

112 Total memory in bytes available on the device, e.g. 1035976704.

113 MAC address of the primary interface. (MAC is different for Wifi and 3G!!)

114 Gyro sensor availabilty, e.g. "Gyro" or "NoGyro".

115 Magnetometer sensor availability, e.g. "Magnetometer" or "NoMagnetometer”.

116 Accelerometer sensor availability, e.g. "Accelerometer" or "NoAccelerometer”.

117 DeviceMotion sensor availability, e.g. "Devicemotion" or "NoDevicemotion”

Android client codes:

201 - Serial number. Required for tablets and exists on some phones.

202 - Android device ID, example: "9774d56d682e549c". On devices after API9, change on factory reset and rooted phones.

203 - WiFi MAC address. Unique but exists only if turned on.
204 - Unique device ID. For example "IMEI" for GSM and "MEID" or "ESN "for CDMA phones. May not exist on some devices.
205 - Simcard number. Exists only on devices with sim card.
206 - Subscriber id. For example "IMSI" for a GSM. May not exist on some devices.
207 - Sim operator name. For example "KPN" or "Vodafone".
208 - Board name. For example "goldfish".
209 - Device manufacturer. For example "HTC" or "Motorola".
210 - Device model. For example: "Nexus One".
211 - API version. For example 10. Changes after system upgrade.
212 - Screen width and height in pixels. For example "240x680".

BlackBerry client codes:
301 - Serial number. Required for tablets and exists on some phones.
302 - BB device ID, example: "9774d56d682e549c". On devices after API9, change on factory reset and rooted phones.
303 - WiFi MAC address. Unique but exists only if turned on.
304 - Unique device ID. For example "IMEI" for GSM and "MEID" or "ESN "for CDMA phones. May not exist on some devices.
305 - Simcard number. Exists only on devices with sim card.
306 - Subscriber id. For example "IMSI" for a GSM. May not exist on some devices.
307 - Sim operator name. For example "KPN" or "Vodafone".
308 - Board name. For example "goldfish".
309 - Device manufacturer. For example "BlackBerry".
310 - Device model. For example: "Q30".
311 - API version. For example 10. Changes after system upgrade.
312 - Screen width and height in pixels. For example "240x680".

Windows Phone client codes:
401 - 499 - reserved for future use.

MacOSX client codes:
501 - 599 - reserved for future use.

Linux client codes:
601 - 699 - reserved for future use.

Some components may or may not be preferred for your setup. Choose those you need or can use. Especially in environments where users for example change local access rights, or make use of dongles/tethering, you may or may not want to enforce one or more of the above mentioned components, such as MAC address.

In some environments it is desirable to prohibit the user to insert anything in the USB socket as this will change the HW signature of that component.

19. Authentication modules

One or more authentication solutions can be connected to the KeyTalk appliance.

As a result you can use your existing infrastructure, without adding a new database.

Of course for testing purposes, or when you only have a small community, an onboard username/password database is available as well.

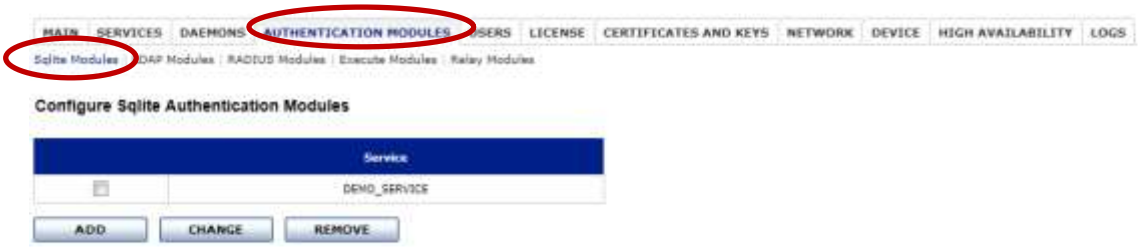
For example, companies with multiple branches, that manage their own authentication solution(s), such as RADIUS or LDAP/AD, can make use of a centrally available KeyTalk to turn their heterogeneous authentication environment into a funneled homogeneous authentication environment.
As a result each company may have their own preferred authentication type, but the network only needs to be configured for one X.509 certificate based solution, making the administration consistent and efficient.

By default KeyTalk has 3 authentication modules onboard. Each module can be used multiple times using its own specific configuration:

- Internal Sqlite based database
- LDAP/AD module
- RADIUS

Companies who wish to bind another type of authentication solution to KeyTalk can make use of our BackEnd API, allowing an easy integration of solutions such as an Oracle or a SQL database.

19.1. Internal Sqlite database module



Configure Sqlite Authentication Modules

	Service
□	DEMO_SERVICE

Figure 51: Configuring the Sqlite authentication modules

The Sqlite Modules section allows you to bind a service to a pre-configured internal database running on the KeyTalk appliance.

Typically this module is used for testing purposes or small user communities.

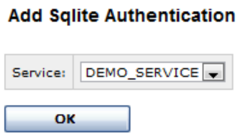
Though more user entries are possible, the maximum amount of users in the Sqlite should not exceed 100, primarily to reduce administrative efforts.

By default the KeyTalk appliance will have the “DEMO_SERVICE” service enabled for testing purposes. The DEMO KeyTalk client RCCD comes pre-configured with this service and the default username “DemoUser”. **This database should be removed prior to taking the KeyTalk appliance into production.**

19.1.1. Adding a Sqlite Module to a service

To add a Sqlite Module to a service, make certain the service exists (i.e. create it) and is not bound to another module.

Choose “ADD” and select one of the available services:



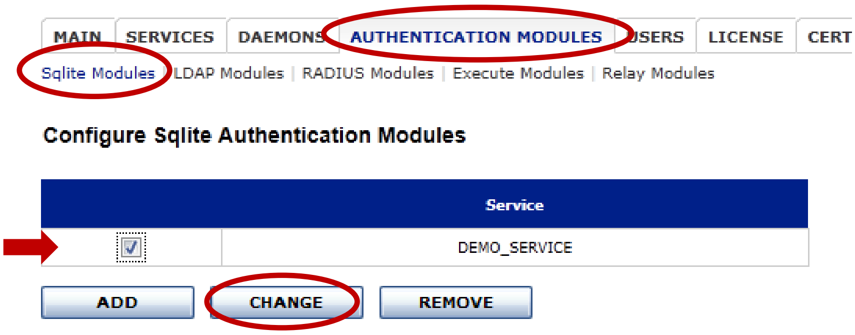
Add Sqlite Authentication Module

Service: DEMO_SERVICE

Figure 52: adding Sqlite Authentication Module

19.1.2. Changing Sqlite Module settings for a service

Go to tab “AUTHENTICATION MODULES”, select “Sqlite modules”, select the service you would like to change and click on “CHANGE”.



Configure Sqlite Authentication Modules

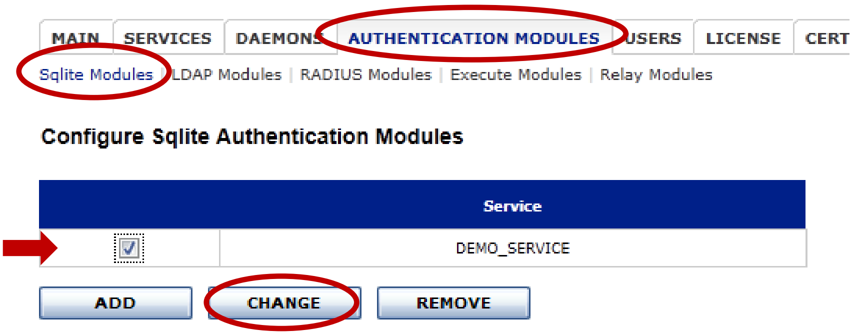
	Service
☑	DEMO_SERVICE

Figure 53: Configuring an Sqlite Authentication module

19.1.2.1. HwSig Verification settings

HwSig (see section 18.2 ‘Hardware Signature’) verification settings allow for the optional configuration of HwSig verification for the specified service.

Go to tab “AUTHENTICATION MODULES”, select “Sqlite modules”, select the service you would like to set the authentication to and click on “CHANGE”.

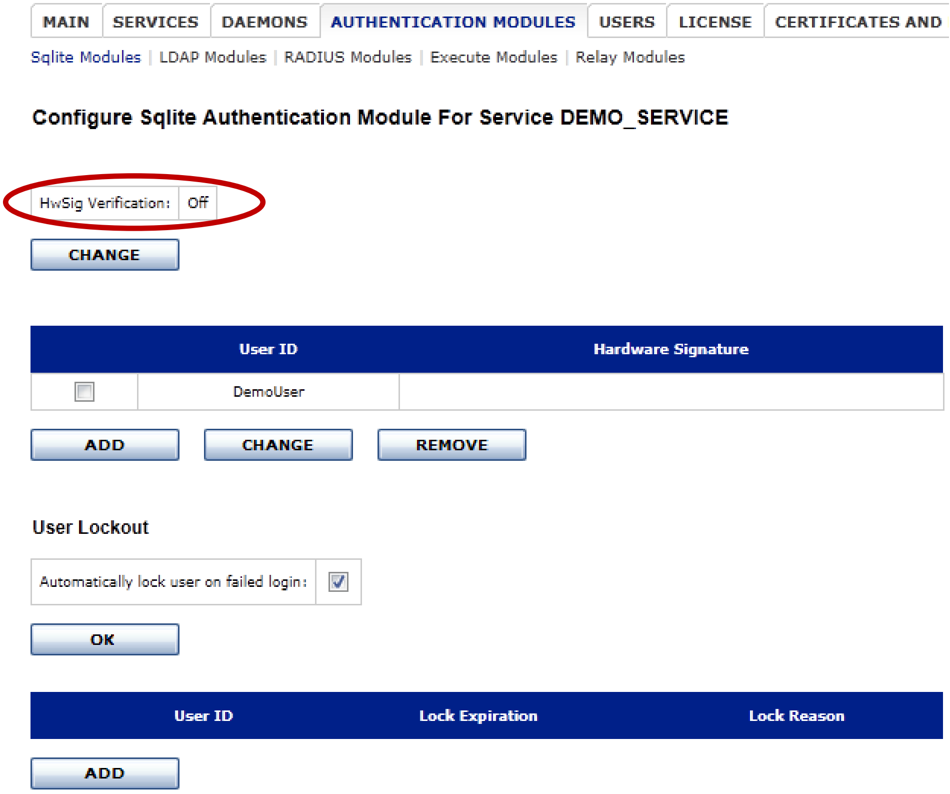

MAIN
SERVICES
DAEMONS
AUTHENTICATION MODULES
USERS
LICENSE
CERT
Sqlite Modules | LDAP Modules | RADIUS Modules | Execute Modules | Relay Modules
ADD
CHANGE
REMOVE

Configure Sqlite Authentication Modules

	Service
☑	DEMO_SERVICE

Figure 54: Configuring an Sqlite Authentication module

The following screen will open:



Configure Sqlite Authentication Module For Service DEMO_SERVICE

HwSig Verification: Off

	User ID	Hardware Signature
□	DemoUser	

User Lockout

Automatically lock user on failed login: ☑

User ID	Lock Expiration	Lock Reason

Figure 55: Configuring Sqlite Authentication module for a specific service

By default the HwSig verification is set to ‘Off’.

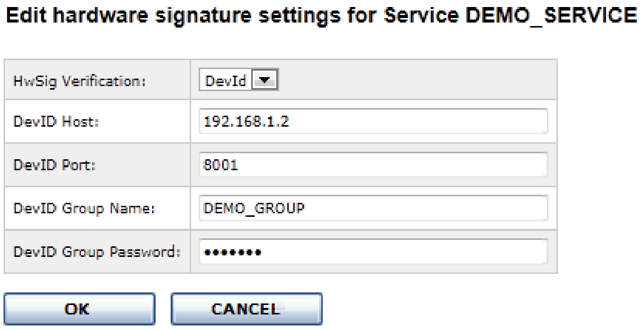
Two other options are available for the HwSig verification:

- DevId: Obtain the user’s HwId from the DevId product solution.

- Exit: Obtain the user’s HwId using the settings of the authentication module.

For the option ‘Exit’, in the case of Sqlite Module, the HwSig is obtained from the user’s Hardware Signature field.

When the ‘DevId’ option has been chosen, ensure that the DevId Host & Port and additional password are properly set.



Edit hardware signature settings for Service DEMO_SERVICE

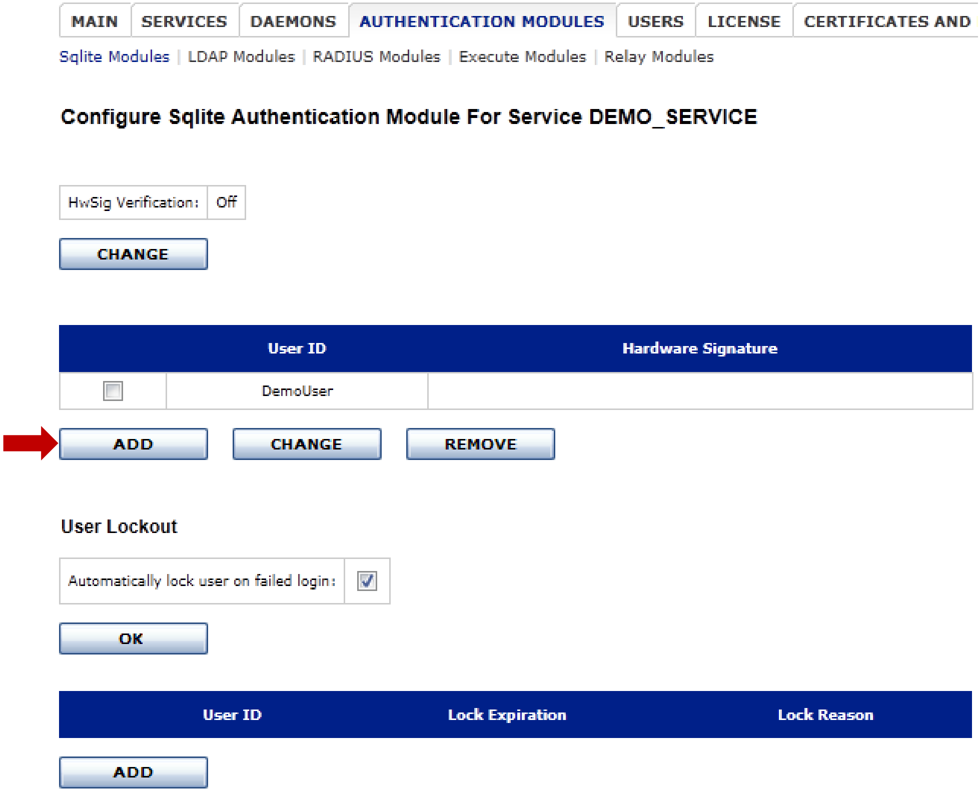
HwSig Verification:	DevId
DevID Host:	192.168.1.2
DevID Port:	8001
DevID Group Name:	DEMO_GROUP
DevID Group Password:	•••••••

Figure 56: Hardware signature set to 'DevId'

19.1.2.2. Add/Change/Remove user

A user can be added, changed or removed:

- Add
  Click on “ADD”.
- Modify
  Select the appropriate user and click on “CHANGE”.
- Delete
  Select the appropriate user(s) and click on “REMOVE”.



Configure Sqlite Authentication Module For Service DEMO_SERVICE

HwSig Verification:	Off

	User ID	Hardware Signature
□	DemoUser	

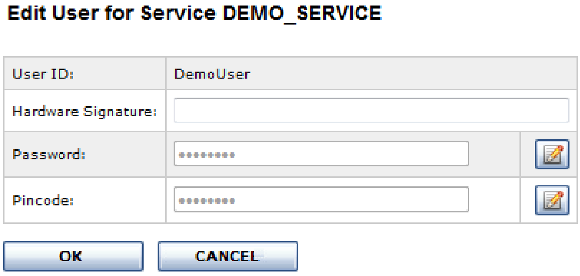
User Lockout

Automatically lock user on failed login:	☑

User ID	Lock Expiration	Lock Reason

Figure 57: Adding/Changing/Removing a user

Adding or changing a user, allows for entering the basic details of a user:



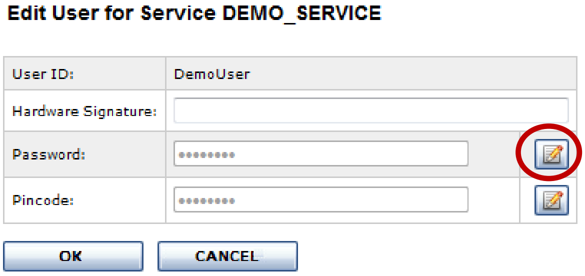
Edit User for Service DEMO_SERVICE

User ID:	DemoUser
Hardware Signature:	
Password:	••••••••
Pincode:	••••••••

Figure 58: Edit user for a specific user belonging to a specific service authentication

Password and pin code will only be verified when configured on the service page!

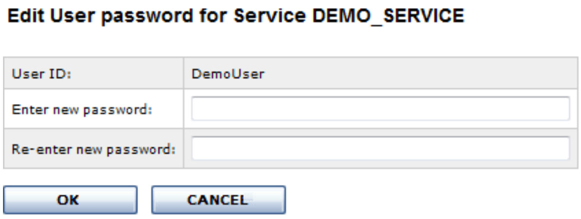
Setting/changing the optional password of a user, requires the selecting of the password “paper-pen”-icon:



Edit User for Service DEMO_SERVICE

User ID:	DemoUser
Hardware Signature:	
Password:	••••••••
Pincode:	••••••••

Figure 59: Setting/Changing a password for a user

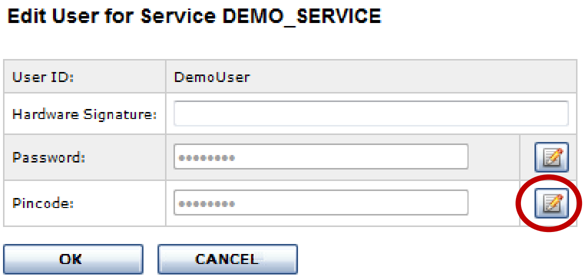


Edit User password for Service DEMO_SERVICE

User ID:	DemoUser
Enter new password:	
Re-enter new password:	

Figure 60: Edit user password

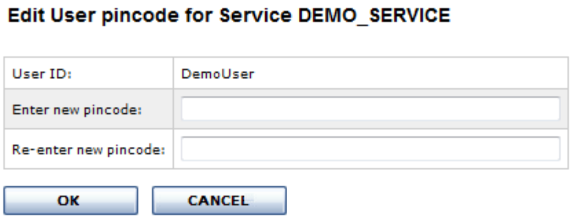
Setting/changing the optional Pincode of a user, requires the selecting of the Pincode "paper-pen"-icon:



Edit User for Service DEMO_SERVICE

User ID:	DemoUser	
Hardware Signature:		
Password:	••••••••	
Pincode:	••••••••	

Figure 61: Setting/Changing the pincode for a user



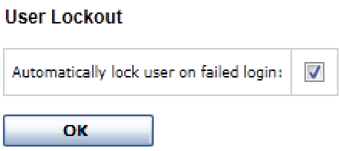
Edit User pincode for Service DEMO_SERVICE

User ID:	DemoUser
Enter new pincode:	
Re-enter new pincode:	

Figure 62: Edit user pincode

19.1.2.3. LockOut

The User LockOut mechanism, allows for users to be temporary suspended from subsequent logins when they enter wrong authentication credentials.



User Lockout

Automatically lock user on failed login:	☑

Figure 63: enable/disable user lockout

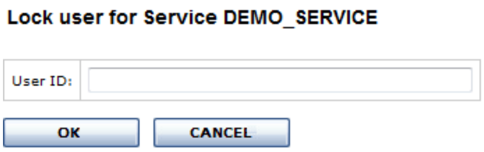
Automatic lockout can be selected or not. Click "OK" to save the settings.

When Automatic lockout is selected, the KeyTalk appliance will add, lock and release users automatically, based on an incremental time penalty.

The Admin can always manually release users before the time penalty expires, AND can manually add or remove users to the LockOut table.

When Automatic lockout is not selected, the system runs in a manual mode, allowing the Admin to add any usernames for a permanent lock, which can only be manually released.

Adding Users manually is done using the user ID. No actual check is performed by the system to see if the User actually exists in the database used by the services' authentication module.

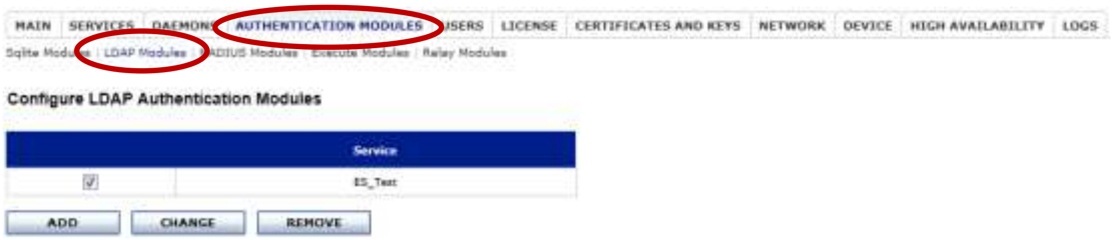

Lock user for Service DEMO_SERVICE

User ID:

Figure 64: Manually adding a user to be locked out for a specific service

19.2. LDAP Module (Includes Active Directory)

The LDAP module allows for Active Directories (AD) and LDAP's alike, to be easily connected to KeyTalk.



Configure LDAP Authentication Modules

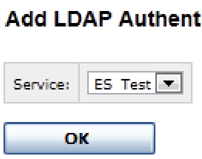
	Service
☑	ES_Test

Figure 65: LDAP Authentication Modules

19.2.1. Adding an LDAP Module

Before adding an LDAP authentication module, a new service must be defined. This service may not be connected to another Authentication Module.

Select "ADD" and select the service you wish to connect:


Add LDAP Authentication Module

Service: ES Test

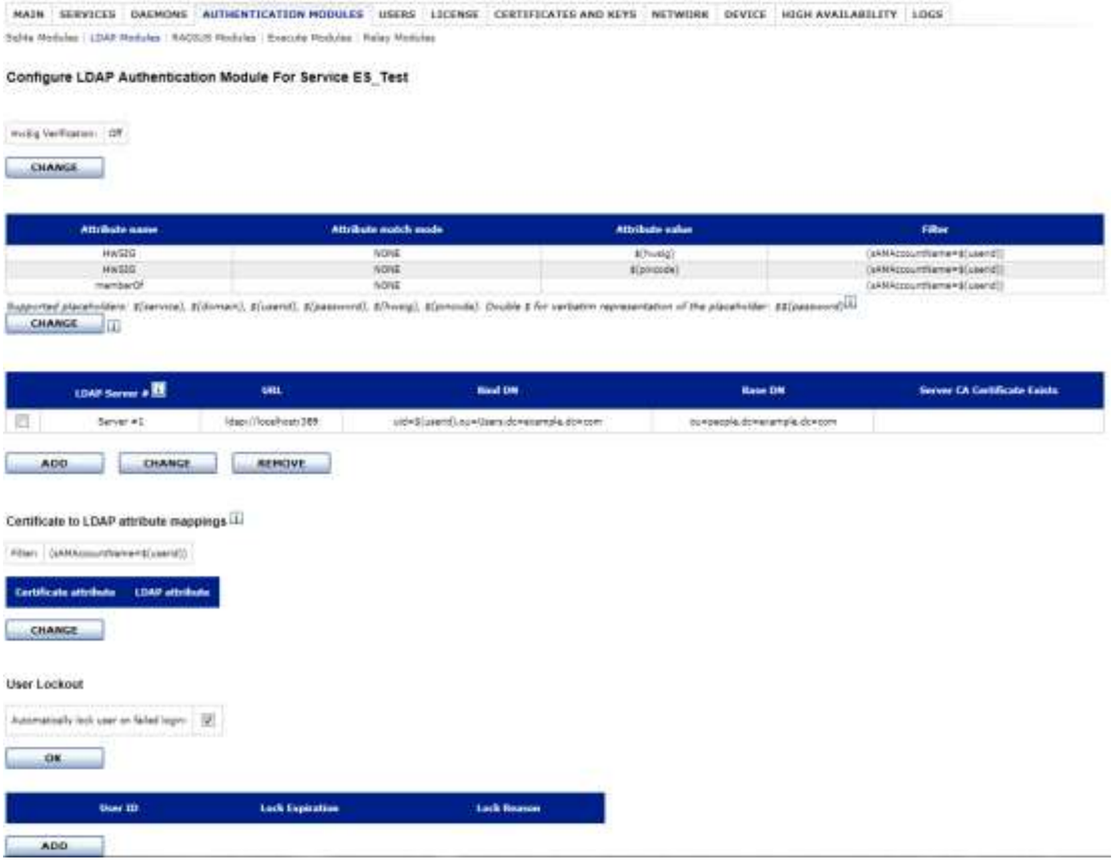
Figure 66: adding an LDAP Authentication Module for a new service named ES Test

Click "OK" to save.

19.2.2. Changing an LDAP Module configuration

To change an LDAP Module configuration of a service, select the appropriate service from the LDAP Configuration Module list, and select “CHANGE”.

This brings up a large overview menu with several different LDAP Module configuration options:



Configure LDAP Authentication Module For Service ES_Test

HwSig Verification: Off

Attribute name	Attribute match mode	Attribute value	Filter
HWSIG	NONE	$(hwsig)	(sAMAccountName=$(userid))
HWSIG	NONE	$(pincode)	(sAMAccountName=$(userid))
memberOf	NONE		(sAMAccountName=$(userid))

Supported placeholders: $(service), $(domain), $(userid), $(password), $(hwsig), $(pincode). Double $ for verbatim representation of the placeholder: $$(password)

	LDAP Server #	URL	Bind DN	Base DN	Server CA Certificate Exists
□	Server #1	ldap://localhost:389	uid=$(userid),ou=Users,dc=example,dc=com	ou=people,dc=example,dc=com	

Certificate to LDAP attribute mappings

Filter: (sAMAccountName=$(userid))

Certificate attribute	LDAP attribute

User Lockout

Automatically lock user on failed login: ☑

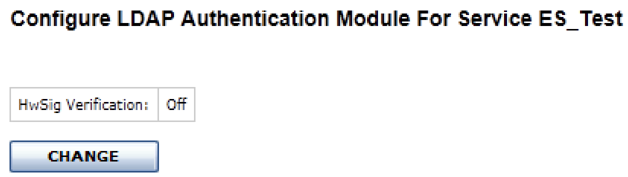
User ID	Lock Expiration	Lock Reason

Figure 67: Configuring LDAP Authentication module for a specific service

19.2.2.1. HwSig Verification settings

HwSig (see section 18.2 'Hardware Signature') verification settings allow for the optional configuration of HwSig verification for the specified service.

By default the HwSig verification is set to 'Off'.



Configure LDAP Authentication Module For Service ES_Test

HwSig Verification:	Off

Figure 68: Hardware Signature verification setting

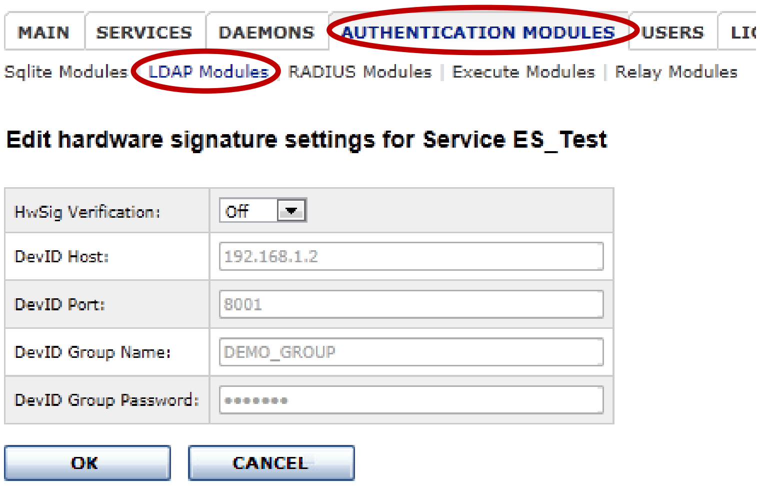
Select "CHANGE" to change the HwSig setting.

Two other options are available for the HwSig verification:

- DevId: Obtain the user's HwId from our DevId product solution.
- Exit: Obtain the user's HwId using the settings of the authentication module.

For the option 'Exit', in the case of LDAP Module, the HwSig is obtained from the user's Hardware Signature field attribute.

When the 'DevId' option has been chosen, make sure that the DevId Host & Port, as well as Group Name and Group password are properly set.



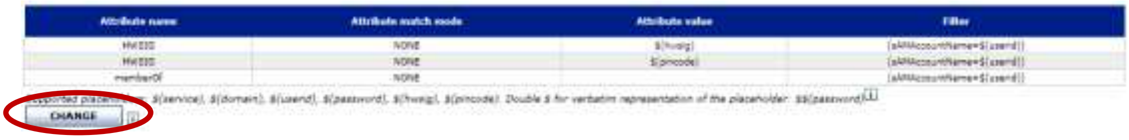
Edit hardware signature settings for Service ES_Test

HwSig Verification:	Off
DevID Host:	192.168.1.2
DevID Port:	8001
DevID Group Name:	DEMO_GROUP
DevID Group Password:	•••••••

Figure 69: Editing Hardware signature settings for a specific service

19.2.2.2. LDAP Attribute Match Settings

To configure the LDAP attribute match settings, choose “CHANGE”.

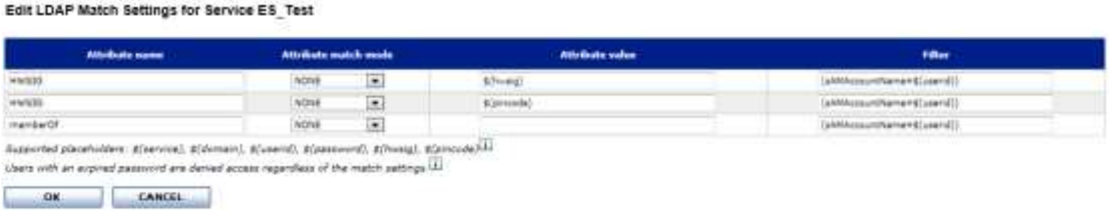


Attribute name	Attribute match mode	Attribute value	Filter
HWSIG	NONE	$(hwsig)	(sAMAccountName=$(userid))
HWSIG	NONE	$(pincode)	(sAMAccountName=$(userid))
memberOf	NONE		(sAMAccountName=$(userid))

Supported placeholders: $(service), $(domain), $(userid), $(password), $(hwsig), $(pincode). Double $ for verbatim representation of the placeholder: $$(password)

Figure 70: LDAP attribute match settings

The following menu will open:



Edit LDAP Match Settings for Service ES_Test

Attribute name	Attribute match mode	Attribute value	Filter
HWSIG	NONE	$(hwsig)	(sAMAccountName=$(userid))
HWSIG	NONE	$(pincode)	(sAMAccountName=$(userid))
memberOf	NONE		(sAMAccountName=$(userid))

Supported placeholders: $(service), $(domain), $(userid), $(password), $(hwsig), $(pincode)

Users with an expired password are denied access regardless of the match settings

Figure 71: Configuring the LDAP attribute match settings

Using LDAP attribute match settings you can set a matching attribute for example to allow for a HardwareSignature to come from your LDAP attribute instead of KeyTalk’s DevID module.

More likely you can use these match settings for nested groups, or to only allow specific members of a security group to be the only ones to obtain a client certificate.

Some examples can be found on the following pages.

This overview explains the different fields and values:

	Attribute name	Attribute match mode		Attribute value	Filter
HwSig	The LDAP attribute name used for storing the Hardware Signature of the user. Default value = HWID	none	HwSig will not be checked	The variable for the HwSig attribute. Placeholders can be used for attribute values which will be substituted with the actual credentials provided by the KeyTalk Client. Supported placeholders are: $(service), $(domain), $(user id), $(password), $(hwsig), $(pincode)	Is the LDAP filter used to specify the record against which the criteria are matched? The filter may also contain the following placeholders which will be substituted with the actual credentials provided by the KeyTalk Client: $(service), $(domain), $(userid), $(password), $(hwsig), $(pincode)
		exact	HwSig needs to match exactly		
		nocaseexact	HwSig must match exactly but not case sensitive		
		subst	HwSig must be a substring of the attribute value		
		nocasesubst	HwSig must be a substring of the attribute value but not case sensitive		
Pincode	The LDAP attribute name used for storing the Pincode of the user. Default value = HWID	none	Pincode will not be checked	The variable for the Pincode attribute. Note: Adding a separator symbol after the variable, can be used to support multiple Pincode's per user. For Example: %PinCode	Is the LDAP filter used to specify the record against which the criteria are matched?
		exact	Pincode needs to match exactly		
		nocaseexact	Pincode must match exactly but not case sensitive		
		subst	Pincode must be a substring of the attribute value		
		nocasesubst	Pincode must be a substring of the attribute value but not case sensitive		
Group	The LDAP attribute name used for storing the Group of the user. Default value = memberOf	none	Group will not be checked	The variable for the Group attribute. Note: Adding a separator symbol after the variable can be used to support multiple Groups per user. For example: Admin	Is the LDAP filter used to specify the record against which the criteria are matched?
		exact	Group needs to match exactly		
		nocaseexact	Group must match exactly but not case sensitive		
		subst	Group must be a substring of the attribute value		
		nocasesubst	Group must be a substring of the attribute value but not case sensitive		

Nested groups

Some companies create Groups within Groups, so called nested Groups.
In accordance with:

http://msdn.microsoft.com/en-us/library/aa746475%28v=vs.85%29.aspx

KeyTalk allows for the use of nested groups, using the syntax:
memberof:1.2.840.113556.1.4.1941:

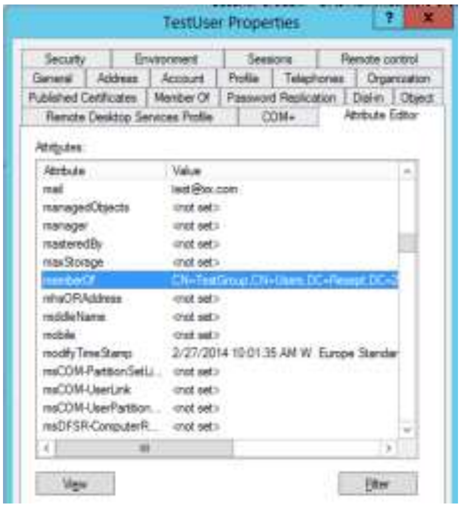
Security groups

It’s very common for companies to assign security group memberships to its users. So when creating a specific BIND you can exclude certain users or devices from obtaining a client certificate when they are not a member of a specific security group.

As an example:
A user is part of the security group “TestGroup”
We can lookup a user his details using:

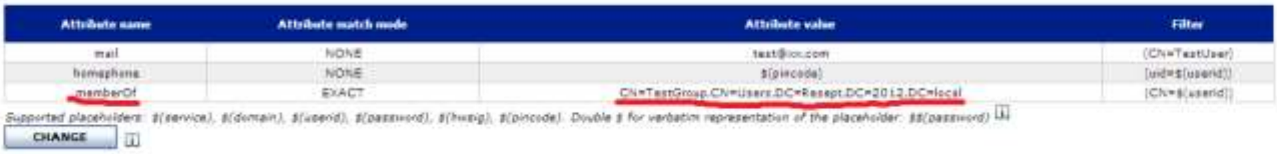
a) Let AD display object attributes: AD snap-in -> menu "View" -> check "Advanced Features"

b) Let AD display the value of memberOf attribute: Go to "TestUser" -> Properties -> "Attribute Editor" -> Filter -> select "backlinks"



Attribute	Value
mail	test@xx.com
managedObjects	<not set>
manager	<not set>
masteredBy	<not set>
maxStorage	<not set>
memberOf	CN=TestGroup,CN=Users,DC=Resept,DC=2
mhsORAddress	<not set>
middleName	<not set>
mobile	<not set>
modifyTimeStamp	2/27/2014 10:01:35 AM W. Europe Standar
msCOM-PartitionSetLi...	<not set>
msCOM-UserLink	<not set>
msCOM-UserPartition...	<not set>
msDFSR-ComputerR...	<not set>

c) Copy memberOf value of the TestUser into the KeyTalk WebUI:



Attribute name	Attribute match mode	Attribute value	Filter
mail	NONE	test@xx.com	(CN=TestUser)
homephone	NONE	$(pincode)	(uid=$(userid))
memberOf	EXACT	CN=TestGroup,CN=Users,DC=Resept,DC=2012,DC=local	(CN=$(userid))

Supported placeholders: $(service), $(domain), $(userid), $(password), $(hwsig), $(pincode). Double $ for verbatim representation of the placeholder: $$(password)

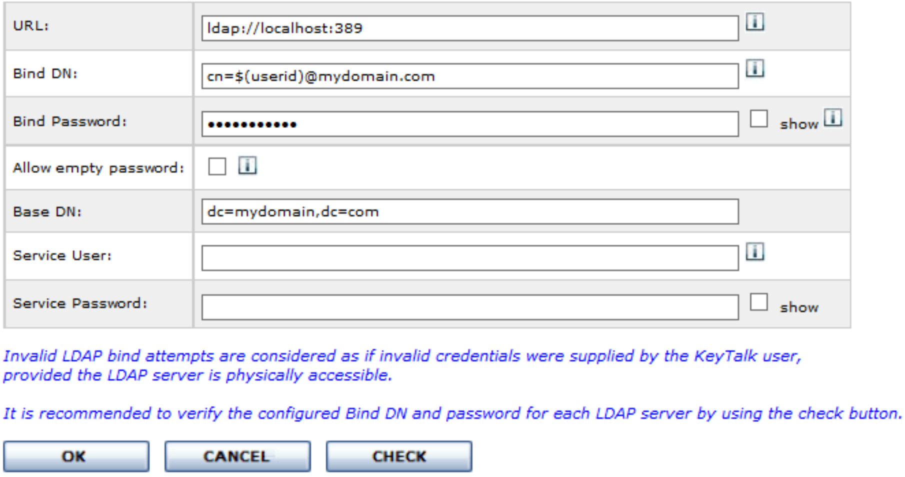
19.2.2.3. Configuring LDAP module Bind & LDAPS for a service

One or multiple LDAP servers can be bound to the KeyTalk appliance.

When the 1st LDAP server cannot be contacted, the KeyTalk appliance will try the 2nd etc.

To verify if the KeyTalk appliance can connect to your LDAP/AD you can optionally (ab)use the ping function under DNS settings.

To configure your LDAP module bind for your selected service: tick the LDAP server configuration entry and select “CHANGE”, or select “ADD”.



URL:	ldap://localhost:389
Bind DN:	cn=$(userid)@mydomain.com
Bind Password:	●●●●●●●●●●● □ show
Allow empty password:	□
Base DN:	dc=mydomain,dc=com
Service User:	
Service Password:	□ show

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 configured Bind DN and password for each LDAP server by using the check button.

Figure 72: Configuring LDAP Server connection

Fieldname	Description
URL	The LDAP location and appropriate port number (for Global Catalog use port 3268).
Bind DN	The Bind DN. Setting appropriate parameters are described in the next sub-chapter.
Bind Password	Either a bind is done using the user’s credentials, or when using anonymous a static password can be provided.
Base DN	The Base DN, usually the same as the BIND DN except without the $(userid) reference
Service User, Service Password	The Service User and Service Password values are used to change the expired password for a user authenticated by Active Directory. When Service User is left empty, it will not be possible to change expired Active Directory passwords. Expiring password still can be changed.

Example:

BIND DN: $(userid)   BASE DN: dc=mydomain, dc=local

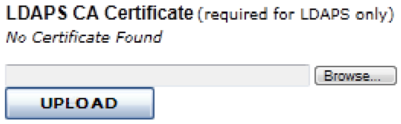
user authenticates with username@domain.local

BASE DN: $(userid)@domain.local BIND DN: dc=mydomain, dc=local

user authenticates with username

To make a secure connection possible between your LDAP/AD and KeyTalk, the LDAPS protocol is supported.

Upload the appropriate CA-tree under which the LDAPS certificate on your AD/LDAP was issued.



LDAPS CA Certificate (required for LDAPS only)

No Certificate Found

Figure 73: Uploading a LDAPS CA Certificate

NOTE 1: The BIND DN and BASE DN are dependent upon the specific LDAP integration.

NOTE 2: When your LDAP certificate is its own Root, LDAPS connections will not work

19.2.2.4. Certificate to LDAP attribute mappings

The X.509 standard defines several fields in a certificate which must be filled in order to be RFC compliant.

By default these certificate fields are filled with the default values as set in the service. When using the default settings, your users will be provided with X.509 user certificates which are all unique based on the date/time of issuing, the serial number, and of course the username.

However, it might be prudent to have more unique user credentials in the certificate. When this is required, you can map your LDAP attributes to the certificate fields.

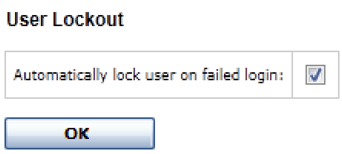
To map the LDAP attributes to the certificate fields: Select “CHANGE” under “Certificate to LDAP attribute mappings“.

Field name	Description	LDAP attribute value
Filter	Is the LDAP filter used to specify the record against which the criteria are matched?	Any valid value
Country	The value of the country code as it should occur in the user certificate.	ISO 3166 standard value
City/Locality	The value of the city/locality as it should occur in the user certificate	Any value, except blank
Organization	The value of the organization as it should occur in the user certificate.	Any value, except blank
Common Name	The value of the Users name as it should occur in the user certificate.	Any value, except blank
Email	The value of the email address as it should occur in the user certificate.	Any value, except blank
Time To Live	The amount of time that a certificate is	Any positive value expressed

	valid from the time it was issued.	in seconds, except blank. Can be 0
Time for Correction	The default time correction factor, expressed in seconds, to correct problems when the Client system time is slightly off.	Any negative value expressed in seconds, except blank. Can be 0 For example: -1800
Basic Constraints	The generated certificate is a user certificate. The generated certificate is a CA certificate and is allowed to issue certificates.	CA:FALSE CA:TRUE
Key Usage	Certificate Key Usage. Values should be comma separated.	digitalSignature nonRepudiation keyEncipherment dataEncipherment keyAgreement
Extended Key Usage	Certificate Extended Key Usage	Refer to: OpenSSL
Subject Alternative Name	The value of the alternative username.	Refer to: OpenSSL

19.2.2.5. User LockOut

The User LockOut mechanism, allows for users to be locked-out from the system when they enter the wrong authentication credentials.



User Lockout

Automatically lock user on failed login: ☑

Figure 74: enable/disable user lockout

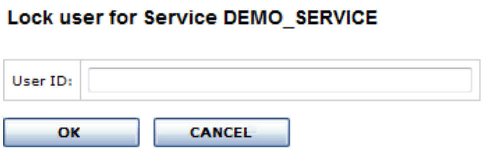
Automatic lockout can be selected or not. Click “OK” to save the settings.

When Automatic lockout is selected, the KeyTalk appliance will add, lock and release users automatically, based on an incremental time penalty.

The Admin can always manually release users before the time penalty expires, AND can manually add or remove users to the LockOut table.

When Automatic lockout is not selected, the system runs in a manual mode, allowing the Admin to add any usernames for a permanent lock, which can only be manually released.

Adding Users manually is done using a free text. No actual check is performed by the system to see if the User actually exists in the database used by the services' authentication module.

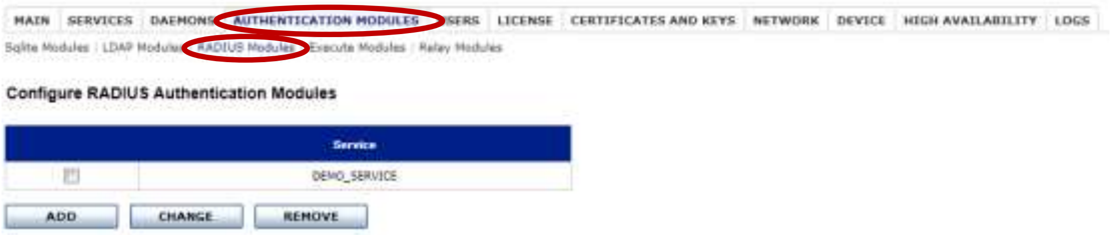


Lock user for Service DEMO_SERVICE

User ID:

Figure 75: Manually adding a user to be locked out for a specific service

19.3. RADIUS Module



Configure RADIUS Authentication Modules

	Service
□	DEMO_SERVICE

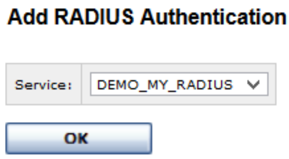
Figure 76: RADIUS Authentication Module

When a RADIUS server is used for authentication purposes, for example when using security tokens, this module can be used to bind the RADIUS based authentication to a KeyTalk service.

19.3.1. Adding a RADIUS Module

To add a RADIUS Module to a service, the service must exist and not be connected to another Authentication Module.

Select "ADD" and select the service you wish to connect:



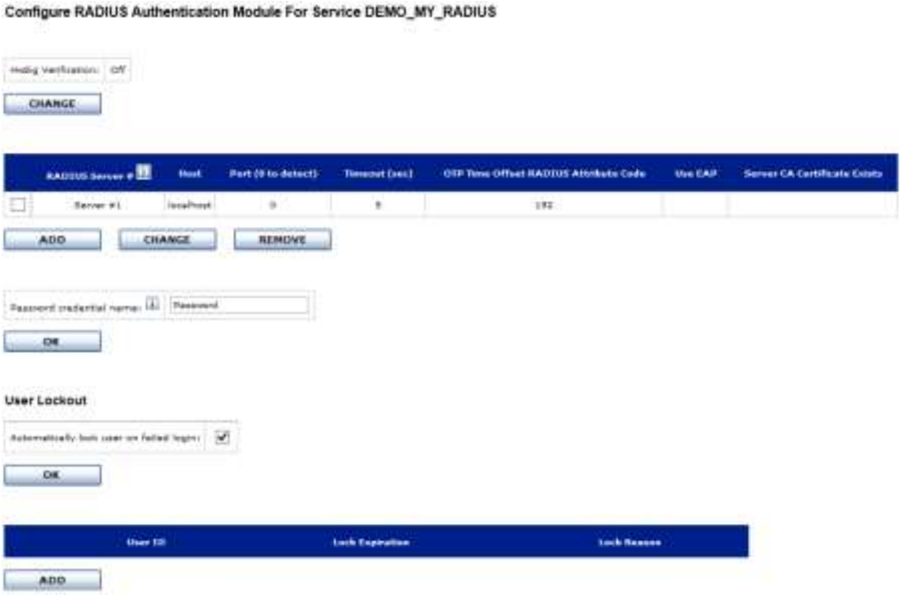
Add RADIUS Authentication Module

Service: DEMO_MY_RADIUS

Figure 77: Adding a RADIUS Authentication Module for service DEMO_MY_RADIUS

19.3.2. Changing a RADIUS Module configuration

To change a RADIUS Module configuration of a service, select the appropriate service from the RADIUS Configuration Module list, and select "CHANGE":



Configure RADIUS Authentication Module For Service DEMO_MY_RADIUS

HwSig Verification: Off

	RADIUS Server #	Host	Port (0 to detect)	Timeout (sec)	OTP Time Offset RADIUS Attribute Code	Use EAP	Server CA Certificate Exists
□	Server #1	localhost	0	5	192		

Password credential name: Password

User Lockout

Automatically lock user on failed login: ☑

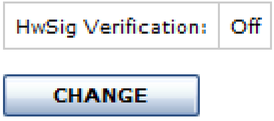
User ID	Lock Expiration	Lock Reason

Figure 78: Configuring the RADIUS Authentication Module for a specified service

19.3.2.1. HwSig Verification settings

HwSig (see section 18.2 'Hardware Signature') verification settings allow for the optional configuration of HwSig verification for the specified service.

By default the HwSig verification is set to 'Off'.



HwSig Verification: Off

Figure 79: Hardware Signature verification setting

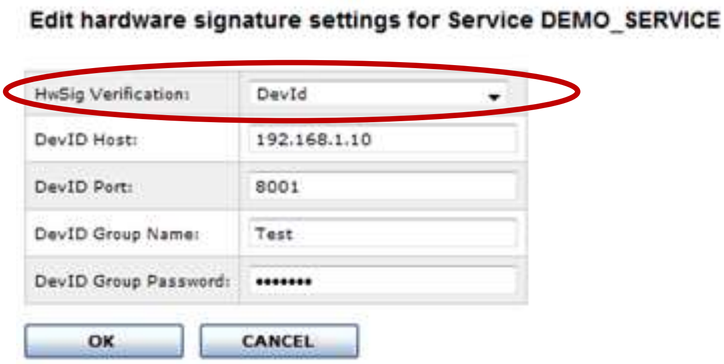
Select "CHANGE" to change the HwSig setting.

Two other options are available for the HwSig verification:

- DevId: Obtain the user's HwId from our DevId product solution.
- Exit: Obtain the user's HwId using the settings of the authentication module.

For the option 'Exit', in the case of Sqlite Module, the HwSig is obtained from the user's Hardware Signature field.

When the ‘DevId’ option has been chosen, make sure that the DevId Host & Port are properly set.



Edit hardware signature settings for Service DEMO_SERVICE

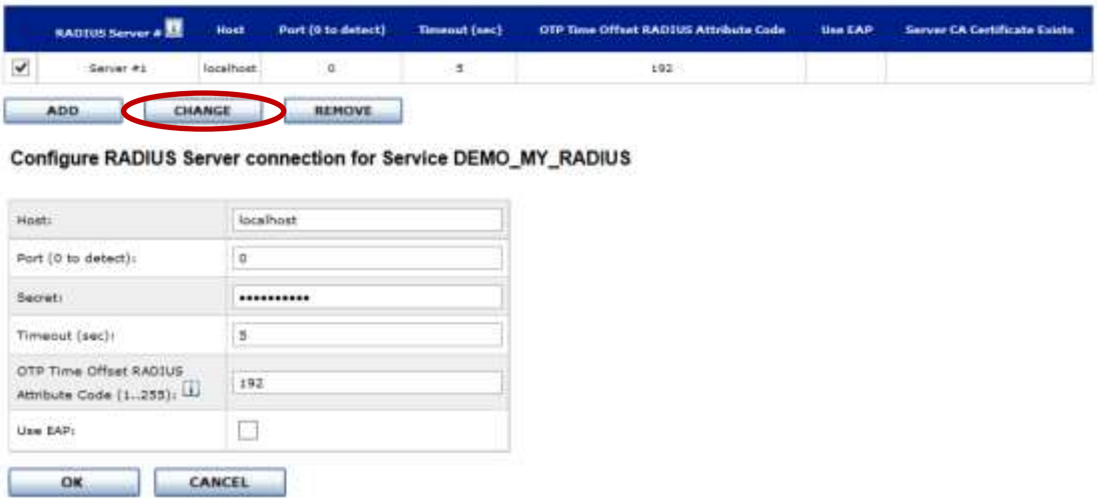
HwSig Verification:	DevId
DevID Host:	192.168.1.10
DevID Port:	8001
DevID Group Name:	Test
DevID Group Password:	•••••••

Figure 80: Editing Hardware signature settings for a specific service

19.3.2.2. RADIUS Server connectivity settings

Multiple RADIUS servers can be configured by selecting the server and clicking on “ADD”. When the fitst server cannot be contacted, the KeyTalk appliance will send its request to the next in line and so forth

To change the RADIUS Server connectivity settings, select the server configuration you wish to change, and click on “CHANGE”.



	RADIUS Server #	Host	Port (0 to detect)	Timeout (sec)	OTP Time Offset RADIUS Attribute Code	Use EAP	Server CA Certificate Exists
☑	Server #1	localhost	0	5	192		

Configure RADIUS Server connection for Service DEMO_MY_RADIUS

Host:	localhost
Port (0 to detect):	0
Secret:	•••••••••••
Timeout (sec):	5
OTP Time Offset RADIUS Attribute Code (1..255):	192
Use EAP:	□

Figure 81: RADIUS server connectivity settings

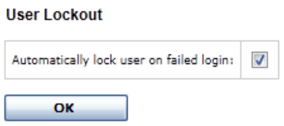
Fieldname	Description	Value
Host	The IP number of the Radius	Any valid IP number
Port (0 to detect)	The communication port number	Any valid port number. Use 0 to have the

		port number automatically detected
Secret	The Radius shared secret	Any valid Radius shared secret
Timeout (sec)	Amount of time assumed for a timeout period before retrying	Any valid positive amount expressed in seconds
OTP Time Offset RADIUS Attribute Code	Code of RADIUS attribute holding the value of time difference between KeyTalk client and KeyTalk server. This attribute is communicated to RADIUS server and is used during One-Time Password (OTP) authentication.	RADIUS attribute code value from 1 to 255
Use EAP	Whether Extended Authentication Protocol (EAP) shall be used to communicate with RADIUS server	Checkbox indicating whether EAP shall be used
EAP Authentication Method	Available when "Use EAP" is selected. The following EAP methods are supported by KeyTalk server aka authenticator: - **Auto-password** When RADIUS server is configured with one of password-based EAP methods (EAP-MD5, LEAP, EAP-MSCHAPv2, EAP-GTC, EAP-TLS, PEAP, EAP-TTLS) the exact method to be used is automatically negotiated between KeyTalk server and RADIUS server. - **PEAP** Use PEAP password-based authentication. For PEAP authentication RADIUS CA certificate is required to verify RADIUS server identity. - **EAP-TTLS** Use EAP-TTLS password-based authentication. For EAP-TTLS authentication RADIUS CA certificate is required to verify RADIUS server identity. - **AKA/SIM** Use EAP-AKA or EAP-SIM challenge-response authentication. The exact method is automatically selected based on card type (UMTS or GSM) supplied by user. Until smartcard support is implemented for the KeyTalk client,	One of "Auto-Password", "PEAP", "EAP-TTLS" or "AKA/SIM" selected from drop-down box.

	smartcard information should be encapsulated in username and encoded as CARD-TYPE_MNC-LENGTh_IMSI. For example: ○ Username GSM_2_354162120787078 indicates that the user provides GSM card with MNC length 2 and IMSI 354162120787078. EAP-SIM method will be selected to authenticate the user ○ - Username UMTS_3_354162120787078 indicates that the user provides UMTS card with MNC length 3 and IMSI 354162120787078. EAP-AKA method will be selected to authenticate the user.	

19.3.2.3. User LockOut

The User LockOut mechanism, allows for users to be locked-out from the system when they enter the wrong authentication credentials.



User Lockout

Automatically lock user on failed login: ☑

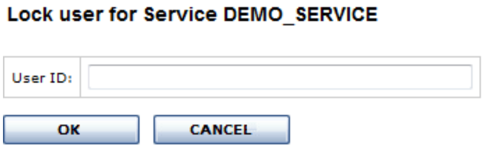
Figure 82: enable/disable user lockout

Automatic lockout can be selected or not. Click “OK” to save the settings.

When Automatic lockout is selected, the KeyTalk appliance will add, lock and release users automatically, based on an incremental time penalty.
The Admin can always manually release users before the time penalty expires, AND can manually add or remove users to the LockOut table.

When Automatic lockout is not selected, the system runs in a manual mode, allowing the Admin to add any usernames for a permanent lock, which can only be manually released.

Adding Users manually is done using a free text. No actual check is performed by the system to see if the User actually exists in the database used by the services’ authentication module.

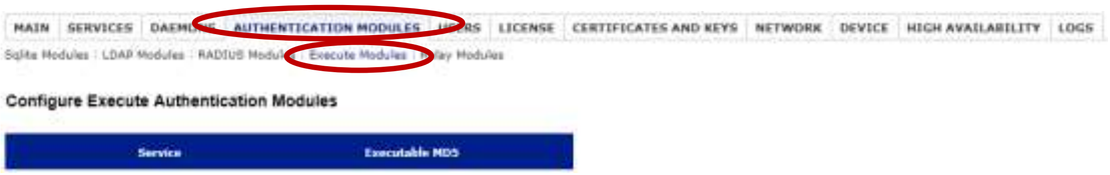


Lock user for Service DEMO_SERVICE

User ID:

Figure 83: Manually adding a user to be locked out for a specific service

19.4. Execute Modules



Configure Execute Authentication Modules

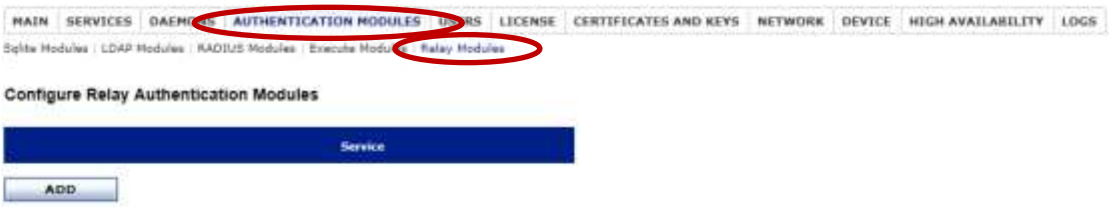
Service	Executable MD5

Figure 84: Executable Authentication Modules

Execute Modules are tailor made modules, officially released by KeyTalk BV as NON-STANDARD. These modules are not part of the formal firmware release but likely will become part of future releases for maintenance purposes.

Though it is not the policy to release modules outside of the officially supported firmware releases, this feature allows for it to be made possible when executing beyond policy. Licensing restrictions may apply. Consult your KeyTalk supplier or partner for more information.

19.5. Relay Modules (connecting other authentication solutions)



Configure Relay Authentication Modules

Service

Figure 85: Relay Authentication Modules

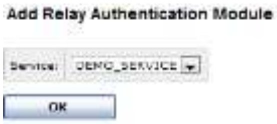
Relay Modules, allow you to make use of the REMAP API, to connect to authentication solutions which are not by default supported by KeyTalk. REMAP: KeyTalk Exit Module Authentication Protocol.

Customers and partners of KeyTalk have made available some unsupported API implementations, which can be requested through your KeyTalk supplier or partner.

19.5.1. Adding a Relay Module

To add a Relay Module to a service, the service must already exist and not be connected to another Authentication Module.

Select “ADD” and select the service you wish to connect:



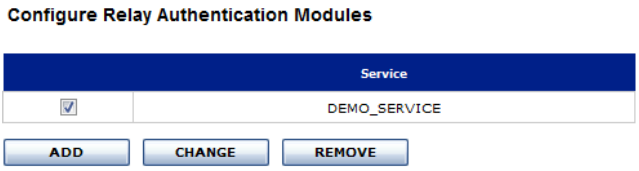
Add Relay Authentication Module

Service: DEMO_SERVICE

Figure 86: Adding a Relay Authentication Module

19.5.2. Changing the Relay Module service configuration

To change the configuration settings, select the Relay Module service for which you wish to change the configuration, and select “CHANGE”.

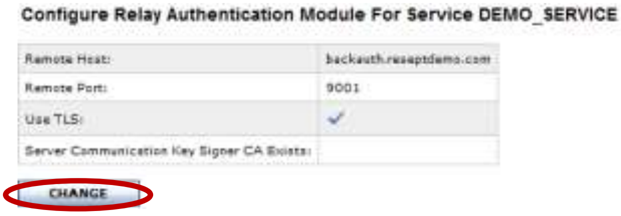


Configure Relay Authentication Modules

	Service
☑	DEMO_SERVICE

Figure 87: Configuring the Relay Authentication Module for a specified service

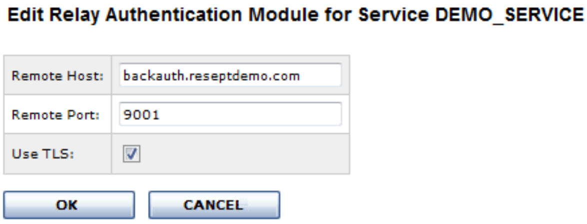
You will now see the current configuration, which can be changed by selecting “CHANGE”.



Configure Relay Authentication Module For Service DEMO_SERVICE

Remote Host:	backauth.reseptdemo.com
Remote Port:	9001
Use TLS:	✓
Server Communication Key Signer CA Exists:	

Figure 88: Current configuration



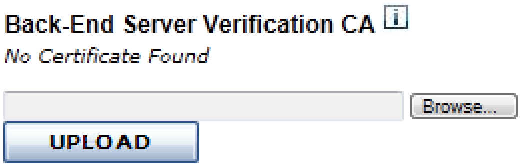
Edit Relay Authentication Module for Service DEMO_SERVICE

Remote Host:	backauth.reseptdemo.com
Remote Port:	9001
Use TLS:	☑

Figure 89: Editing the configuration

Since the Relay module effectively makes use of a host running remote, only a connection needs to be defined for the Remote Host.

Configure the Remote Host and corresponding Port and whether or not TLS should be used to secure the communication.


Back-End Server Verification CA

No Certificate Found

Figure 90: For TLS a server communication key signer CA certificate is needed

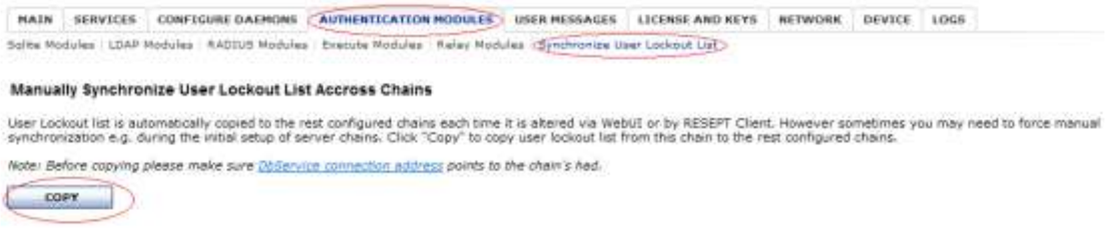
Additionally when using SSL/TLS you will need to upload the Server Communication Key Signer CA certificate in PEM format. This does NOT need to be a certificate created under your Certificate Authority tree, but can also be that of a 3rd party, such as VeriSign, or Microsoft.

19.5.3. Remote exit basics

When you wish to create your own authentication module (exit), you should always run it from a separate server.

The details of what needs to be configured are covered in a separate Remote Exit document which is available through your KeyTalk supplier or partner.

19.6. Synchronize User Lockout List



Manually Synchronize User Lockout List Accross Chains

User Lockout list is automatically copied to the rest configured chains each time it is altered via WebUI or by RESEPT Client. However sometimes you may need to force manual synchronization e.g. during the initial setup of server chains. Click "Copy" to copy user lockout list from this chain to the rest configured chains.

Note: Before copying please make sure DbService connection address points to the chain's had.

Figure 91: Synchronize user lockout list

This functionality is only applicable when running KeyTalk in a high availability configuration.

This feature allows you to manually initialize a synchronization of all your User Lockout Lists from all your Authentication Modules for all services on the KeyTalk appliance.

HA will automatically synchronize, but the manual feature is meant for synchronization after adding a new system to your High Availability setup.

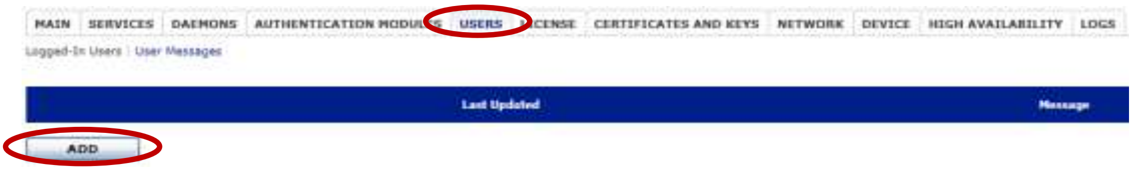
20. User messages and User accounting

20.1. User messages

User messages allow the Organization's administrator to send a custom message to the user when their KeyTalk client authenticates.

A common usage would be to inform users of network downtime announcements for example.

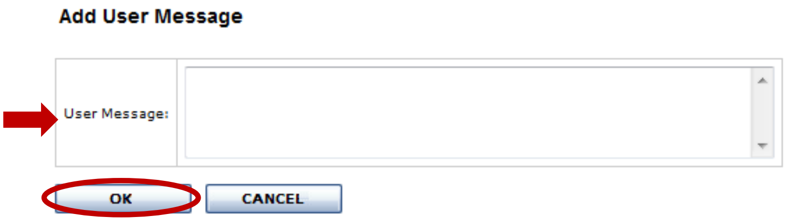
To create a user message, select "USERS" from the main menu and click on "ADD".



Last Updated	Message

Figure 92: Adding a user message

Type the message that needs to be sent to all users with a KeyTalk Client and click "OK" to make the message available to your user community.

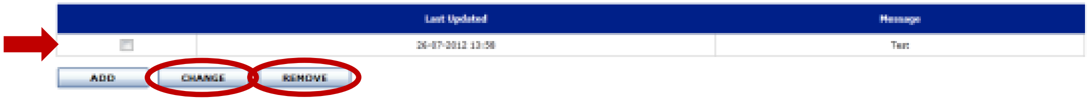


Add User Message

User Message:

Figure 93: Adding user message and making it available to the KeyTalk Client users

An existing user message can be changed or removed by selecting the user message and clicking on "CHANGE" or "REMOVE".

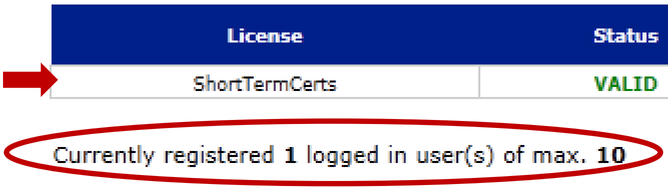


	Last Updated	Message
□	26-07-2012 13:58	Test

Figure 94: Changing or removing a user message

20.2. Logged-in Users

You can check if your license is still valid. Additionally, your license capability to serve a number of users can also be checked per service on the “MAIN” tab of KeyTalk.

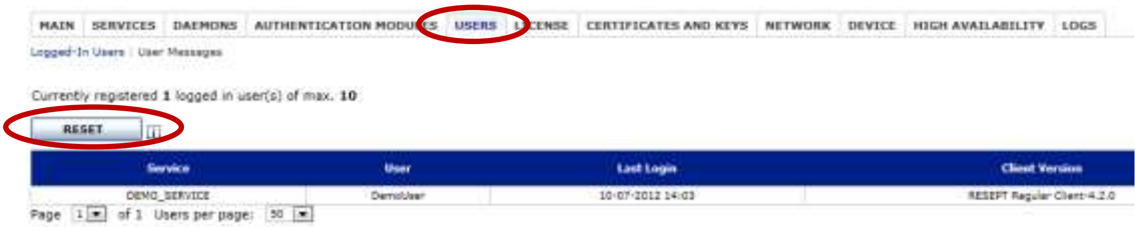


License	Status
ShortTermCerts	VALID

Currently registered **1** logged in user(s) of max. **10**

Figure 95: License validity and number of users logged in

It is possible that some users have left your company, but are still counted as ‘logged in users’. To correct the user-counter field the “RESET” button on the “USERS” tab can be clicked, deleting the 10% of users that did not log in recently (oldest first).



Currently registered **1** logged in user(s) of max. **10**

Service	User	Last Login	Client Version
DEMO_SERVICE	DemoUser	10-07-2012 14:03	RESEPT Regular Client-4.2.0

Page 1 of 1 Users per page: 50

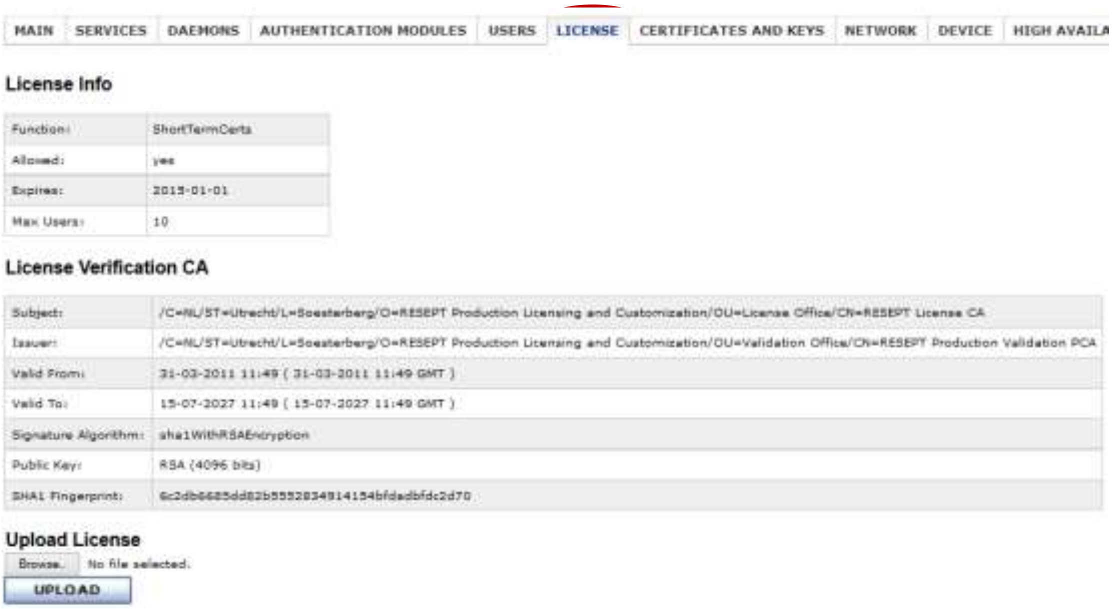
Figure 96: Resetting the oldest 10% of counted users

Deleting this 10% of oldest counted users can also be done via the LCD menu of the physical appliance. See section 24 ‘LCD information display’ for more information.

21. KeyTalk Appliance License

The KeyTalk Appliance License file contains your company name text in a text file format. Your contract details apply. It is personalized to your company and contains all the information required to make the (virtual) appliance work.

Your license details can be viewed under the “License” tab.



License Info

Function:	ShortTermCerts
Allowed:	yes
Expires:	2015-01-01
Max Users:	10

License Verification CA

Subject:	/C=NL/ST=Utrecht/L=Soesterberg/O=RESEPT Production Licensing and Customization/OU=License Office/CN=RESEPT License CA
Issuer:	/C=NL/ST=Utrecht/L=Soesterberg/O=RESEPT Production Licensing and Customization/OU=Validation Office/CN=RESEPT Production Validation PCA
Valid From:	31-03-2011 11:49 (31-03-2011 11:49 GMT)
Valid To:	15-07-2027 11:49 (15-07-2027 11:49 GMT)
Signature Algorithm:	sha1WithRSAEncryption
Public Key:	RSA (4096 bits)
SHA1 Fingerprint:	6c2db6685dd82b5552834914154bfdadbfdc2d70

Upload License

Browse... No file selected.

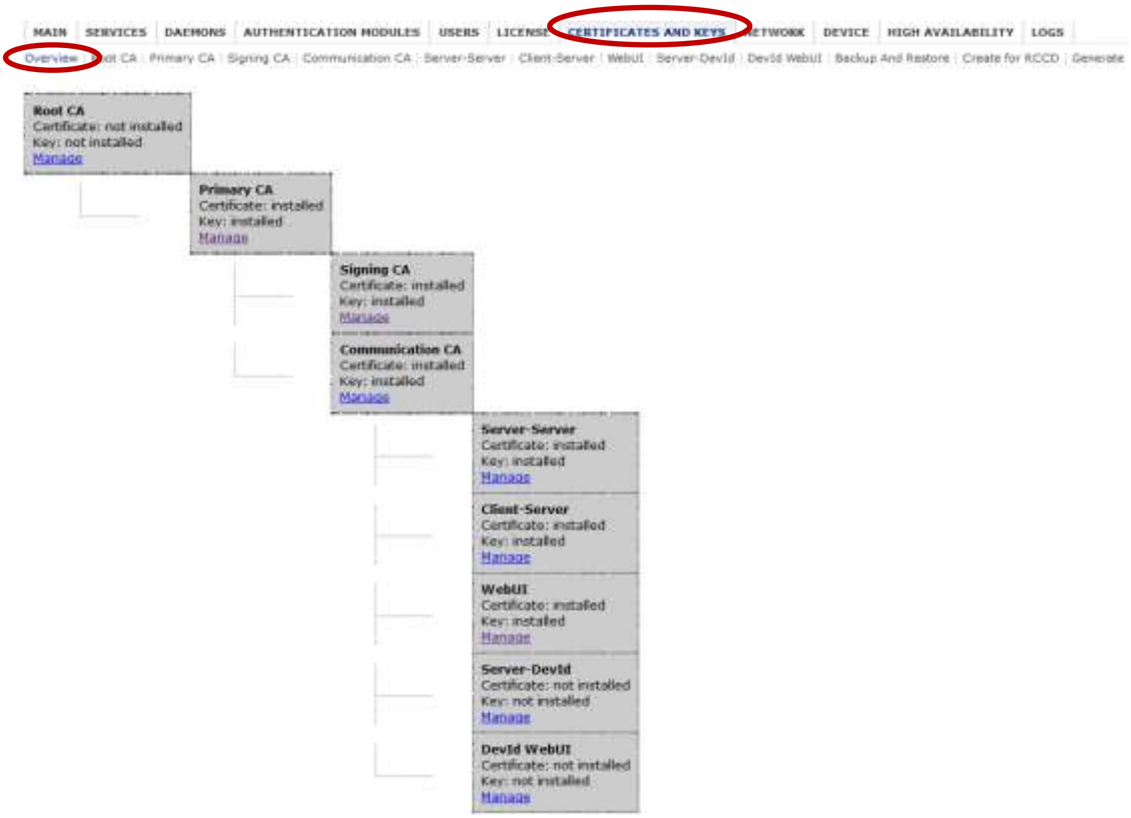
Figure 97: View license info or upload a new license

A new license can be uploaded by selecting the license via “Browse…” and clicking “UPLOAD”.

The text file is signed by KeyTalk, ensuring that any tampered text files cannot be uploaded as a valid license. The maximum amount of users refers to the maximum amount of unique usernames used to obtain a certificate in a given timeframe.

22. Certificates and keys

On the “CERTIFICATE AND KEYS” tab the Certificate Authority Keys for the KeyTalk appliance can be managed.



Root CA
Certificate: not installed
Key: not installed
Manage

Primary CA
Certificate: installed
Key: installed
Manage

Signing CA
Certificate: installed
Key: installed
Manage

Communication CA
Certificate: installed
Key: installed
Manage

Server-Server
Certificate: installed
Key: installed
Manage

Client-Server
Certificate: installed
Key: installed
Manage

WebUI
Certificate: installed
Key: installed
Manage

Server-DevId
Certificate: not installed
Key: not installed
Manage

DevId WebUI
Certificate: not installed
Key: not installed
Manage

Figure 98: Overview of the KeyTalk Certificate Authority

By default your KeyTalk appliance comes pre-configured with demo key and certificate material. This material is NOT unique, but provided with every system. It is therefore necessary to be replaced by your own material when going into production. The demo material can be used for testing or KeyTalk’s free trial.

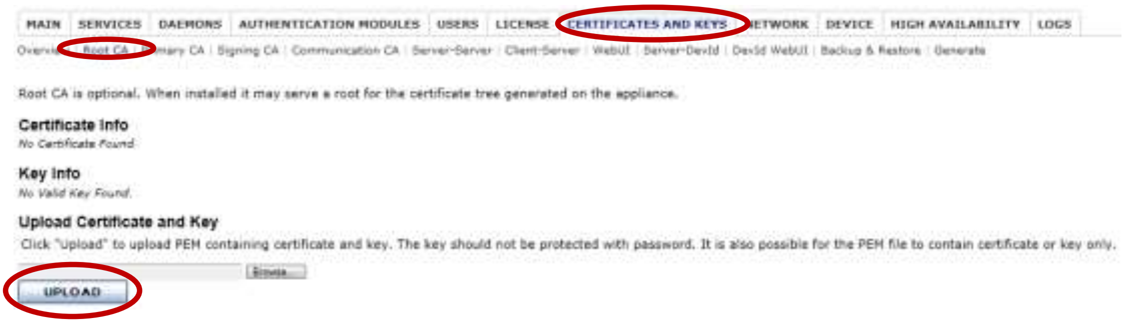
KeyTalk requires the certificates to be imported or generated in PEM file format and requires that they contain the .pem file extension.

Please note that the KeyTalk solution does not mandatorily require you to take into account any specific protocols and procedures as to the security level of key-creation, key management, etc. Instead it is your company who decides what is and what is not acceptable.

22.1. Root CA

The Root CA is an optional public certificate. It is only applicable when your company already has an existing certificate authority in place.

When installed it may serve as a root for the certificate tree generated on the appliance.



Root CA is optional. When installed it may serve a root for the certificate tree generated on the appliance.

Certificate Info

No Certificate Found

Key Info

No Valid Key Found.

Upload Certificate and Key

Click "Upload" to upload PEM containing certificate and key. The key should not be protected with password. It is also possible for the PEM file to contain certificate or key only.

Figure 99: Root CA information and key upload functionality

A new certificate can be uploaded by selecting it via “Browse…” and clicking “UPLOAD”.

After a successful UPLOAD the device management subsystem will automatically restart to effectuate the new certificate.

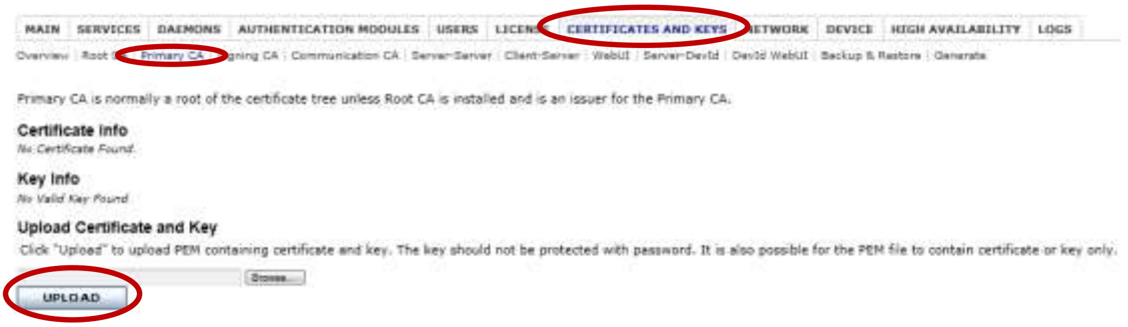
To make the changes permanent, please refer to section 8.2 ‘Saving changes & reboot’.

22.2. Primary CA

The Primary CA is a private key and is normally a root of the certificate tree unless the Root CA is installed and is an issuer for the Primary CA.

After generation this key is kept offline and is usually stored on a portable media in your safe. Depending on your security requirements it can be distributed in parts, for safe keeping, among several custodians.

This file also contains the Primary CA Certificate in PEM format.



Primary CA is normally a root of the certificate tree unless Root CA is installed and is an issuer for the Primary CA.

Certificate Info

No Certificate Found.

Key Info

No Valid Key Found

Upload Certificate and Key

Click "Upload" to upload PEM containing certificate and key. The key should not be protected with password. It is also possible for the PEM file to contain certificate or key only.

Figure 100: Primary CA information and key upload functionality

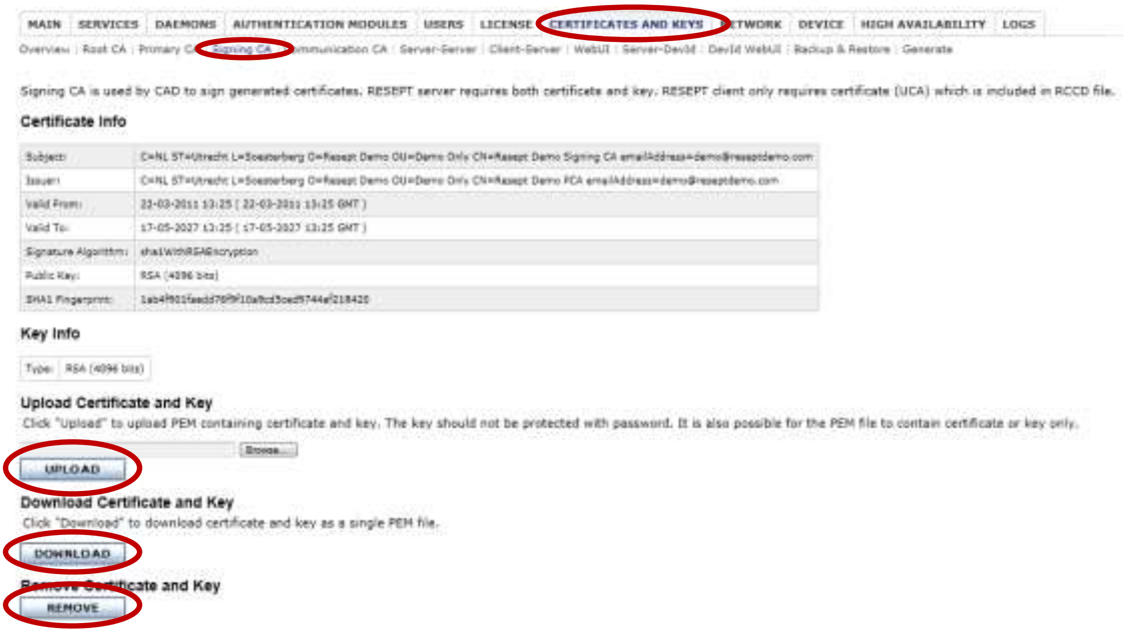
A new certificate can be uploaded by selecting it via “Browse…” and clicking “UPLOAD”.

After a successful UPLOAD the device management subsystem will automatically restart to effectuate the new certificate.

To make the changes permanent, please refer to section 8.2 ‘Saving changes & reboot’.

22.3. Signing CA

This tab allows you to upload your own signing certificate and key, used to issue user certificates and keys. When you have a separate key and certificate you can upload these individually and KeyTalk will combine them for you.


MAIN
SERVICES
DAEMONS
AUTHENTICATION MODULES
USERS
LICENSE
CERTIFICATES AND KEYS
NETWORK
DEVICE
HIGH AVAILABILITY
LOGS
Overview | Root CA | Primary CA | Signing CA | Communication CA | Server-Server | Client-Server | WebUI | Server-DevId | DevId WebUI | Backup & Restore | Generate

Signing CA is used by CAD to sign generated certificates. RESEPT server requires both certificate and key. RESEPT client only requires certificate (UCA) which is included in RCCD file.

Certificate Info

Subject:	C=NL ST=Utrecht L=Soesterberg O=Resept Demo OU=Demo Only CN=Resept Demo Signing CA emailAddress=demo@reseptdemo.com
Issuer:	C=NL ST=Utrecht L=Soesterberg O=Resept Demo OU=Demo Only CN=Resept Demo PCA emailAddress=demo@reseptdemo.com
Valid From:	22-03-2011 13:25 (22-03-2011 13:25 GMT)
Valid To:	17-05-2027 13:25 (17-05-2027 13:25 GMT)
Signature Algorithm:	sha1WithRSAEncryption
Public Key:	RSA (4096 bits)
SHA1 Fingerprint:	1ab4f901faedd76f9f10a8cd3oed9744ef218420

Key Info

Type:	RSA (4096 bits)

Upload Certificate and Key

Click "Upload" to upload PEM containing certificate and key. The key should not be protected with password. It is also possible for the PEM file to contain certificate or key only.

Download Certificate and Key

Click "Download" to download certificate and key as a single PEM file.

Remove Certificate and Key

Figure 101: Signing CA information and key upload functionality

This screen allows you to download and remove the current certificate and key, and upload a new version.

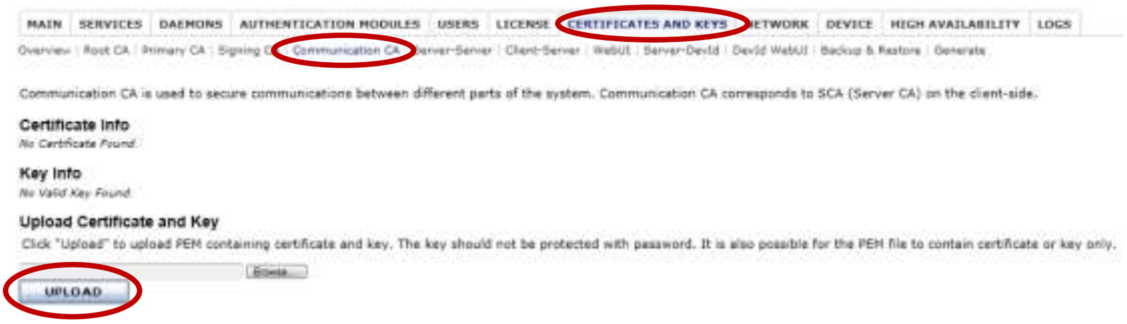
A new certificate can be uploaded by selecting it via “Browse…” and clicking “UPLOAD”.

After a successful UPLOAD the device management subsystem will automatically restart to effectuate the new certificate.

To make the changes permanent, please refer to section 8.2 ‘Saving changes & reboot’.

22.4. Communication CA

This tab is used to secure communications between different parts of the system. The Communication CA corresponds to the SCA (Server CA) on the client-side.


MAIN
SERVICES
DAEMONS
AUTHENTICATION MODULES
USERS
LICENSE
CERTIFICATES AND KEYS
NETWORK
DEVICE
HIGH AVAILABILITY
LOGS
Overview | Root CA | Primary CA | Signing CA | Communication CA | Server-Server | Client-Server | WebUI | Server-DevId | DevId WebUI | Backup & Restore | Generate
Browse...
UPLOAD

Communication CA is used to secure communications between different parts of the system. Communication CA corresponds to SCA (Server CA) on the client-side.

Certificate Info

No Certificate Found.

Key Info

No Valid Key Found.

Upload Certificate and Key

Click "Upload" to upload PEM containing certificate and key. The key should not be protected with password. It is also possible for the PEM file to contain certificate or key only.

Figure 102: Communication CA information and key upload functionality

A new certificate can be uploaded by selecting it via “Browse…” and clicking “UPLOAD”.

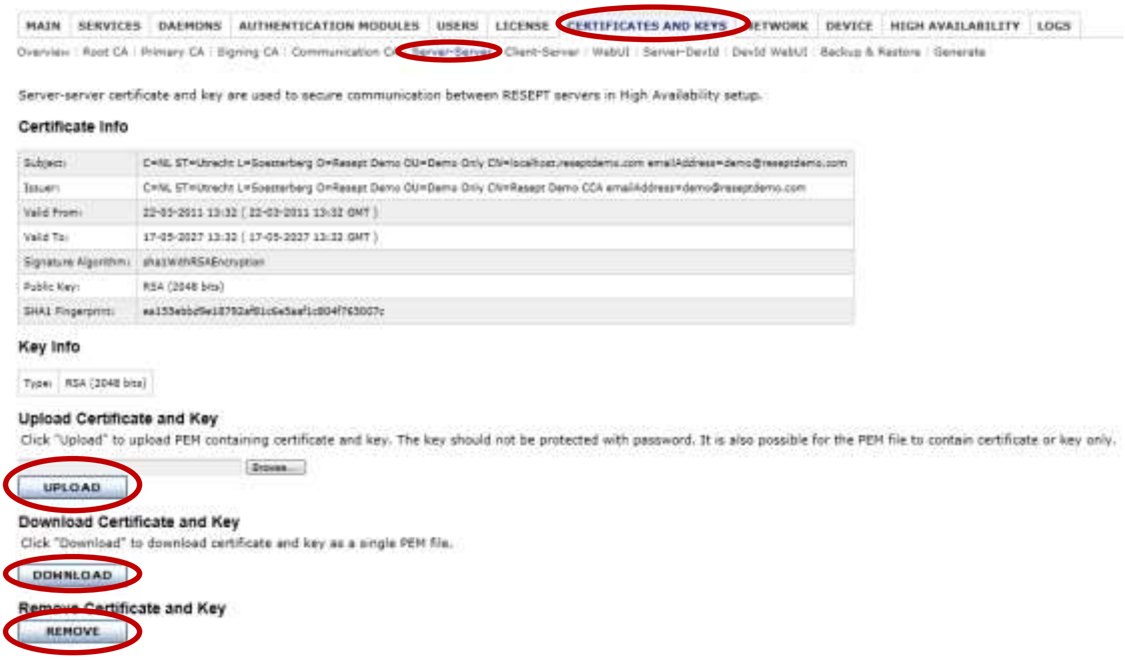
After a successful UPLOAD the device management subsystem will automatically restart to effectuate the new certificate.

To make the changes permanent, please refer to section 8.2 ‘Saving changes & reboot’.

22.5. Server-Server Communication Key

This tab allows you to view the information of the Server-Server Communication Key and certificate.

This certificate and key is required to encrypt the information exchange between KeyTalk servers in High Availability mode; For KeyTalk’s DevID appliance we have a separate menu item “Server-Devid”
You can upload the combined certificate and key as a single file or you can upload the key and the certificate as separate files in PEM format. There is no need to rename the files, as KeyTalk will do this for you.


MAIN
SERVICES
DAEMONS
AUTHENTICATION MODULES
USERS
LICENSE
CERTIFICATES AND KEYS
NETWORK
DEVICE
HIGH AVAILABILITY
LOGS
Overview | Root CA | Primary CA | Signing CA | Communication CA | Server-Server | Client-Server | WebUI | Server-DevId | DevId WebUI | Backup & Restore | Generate

Server-server certificate and key are used to secure communication between RESEPT servers in High Availability setup.

Certificate Info

Subject:	C=NL ST=Utrecht L=Soesterberg O=Resept Demo OU=Demo Only CN=localhost.reseptdemo.com emailAddress=demo@reseptdemo.com
Issuer:	C=NL ST=Utrecht L=Soesterberg O=Resept Demo OU=Demo Only CN=Resept Demo CCA emailAddress=demo@reseptdemo.com
Valid From:	22-03-2011 13:32 (22-03-2011 13:32 GMT)
Valid To:	17-05-2027 13:32 (17-05-2027 13:32 GMT)
Signature Algorithm:	sha1WithRSAEncryption
Public Key:	RSA (2048 bits)
SHA1 Fingerprint:	ea133ebbd9e18792af81c6e5aaf1c804f763007c

Key Info

Type:	RSA (2048 bits)

Upload Certificate and Key

Click "Upload" to upload PEM containing certificate and key. The key should not be protected with password. It is also possible for the PEM file to contain certificate or key only.

Download Certificate and Key

Click "Download" to download certificate and key as a single PEM file.

Remove Certificate and Key

Figure 103: Server-server certificate information and key upload functionality

This screen allows you to download and remove the current certificate and key, and upload a new version.

A new certificate can be uploaded by selecting it via “Browse…” and clicking “UPLOAD”.

After a successful UPLOAD the device management subsystem will automatically restart to effectuate the new certificate.

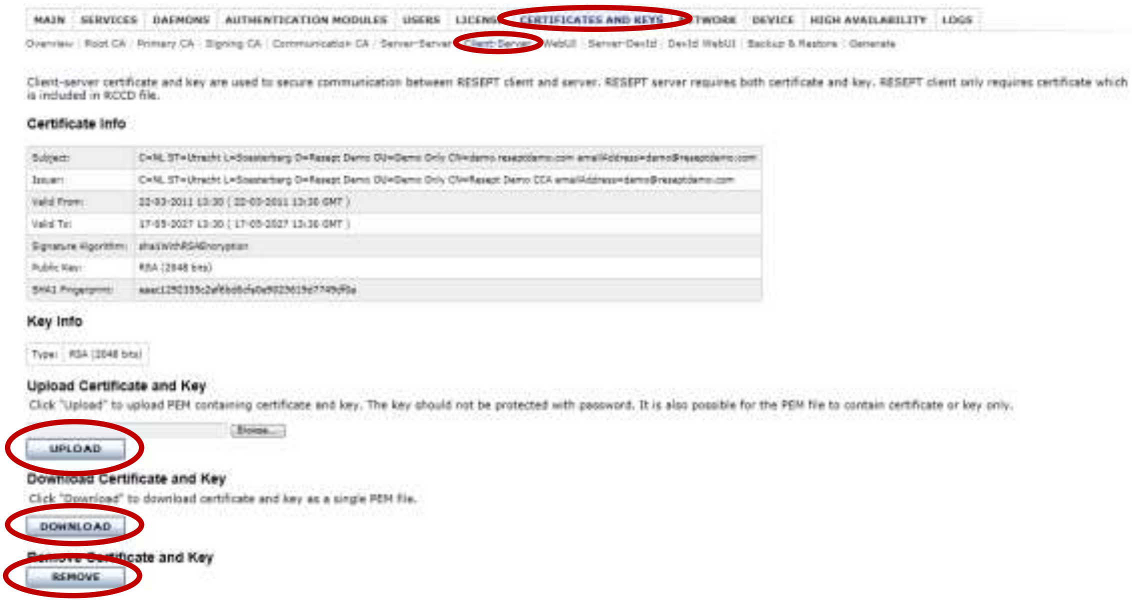
To make the changes permanent, please refer to section 8.2 ‘Saving changes & reboot’.

22.6. Client-Server Communication Key

This tab allows you to view the information of the KeyTalk Client-Server Key and certificate.

This certificate and key is required to establish a secure connection between the KeyTalk client and the KeyTalk server.

You can upload the combined certificate and key as a single file or you can upload the key and the certificate as separate files in PEM format. There is no need to rename the files, as KeyTalk will do this for you.


MAIN
SERVICES
DAEMONS
AUTHENTICATION MODULES
USERS
LICENSE
CERTIFICATES AND KEYS
NETWORK
DEVICE
HIGH AVAILABILITY
LOGS
Overview | Root CA | Primary CA | Signing CA | Communication CA | Server-Server | Client-Server | WebUI | Server-DevId | DevId WebUI | Backup & Restore | Generate

Client-server certificate and key are used to secure communication between RESEPT client and server. RESEPT server requires both certificate and key. RESEPT client only requires certificate which is included in RCCD file.

Certificate Info

Subject:	C=NL ST=Utrecht L=Soesterberg O=Resept Demo OU=Demo Only CN=demo.reseptdemo.com emailAddress=demo@reseptdemo.com
Issuer:	C=NL ST=Utrecht L=Soesterberg O=Resept Demo OU=Demo Only CN=Resept Demo CCA emailAddress=demo@reseptdemo.com
Valid From:	22-03-2011 13:30 (22-03-2011 13:30 GMT)
Valid To:	17-03-2027 13:30 (17-03-2027 13:30 GMT)
Signature Algorithm:	sha1WithRSAEncryption
Public Key:	RSA (2048 bits)
SHA1 Fingerprint:	aaac1292335c2af6bd6cfa0e9023619e7749cf9a

Key Info

Type:	RSA (2048 bits)

Upload Certificate and Key

Click "Upload" to upload PEM containing certificate and key. The key should not be protected with password. It is also possible for the PEM file to contain certificate or key only.

Download Certificate and Key

Click "Download" to download certificate and key as a single PEM file.

Remove Certificate and Key

Figure 104: Client-server certificate information and key upload functionality

This screen allows you to download and remove the current certificate and key, and upload a new version.

A new certificate can be uploaded by selecting it via “Browse…” and clicking “UPLOAD”.

After a successful UPLOAD the device management subsystem will automatically restart to effectuate the new certificate.

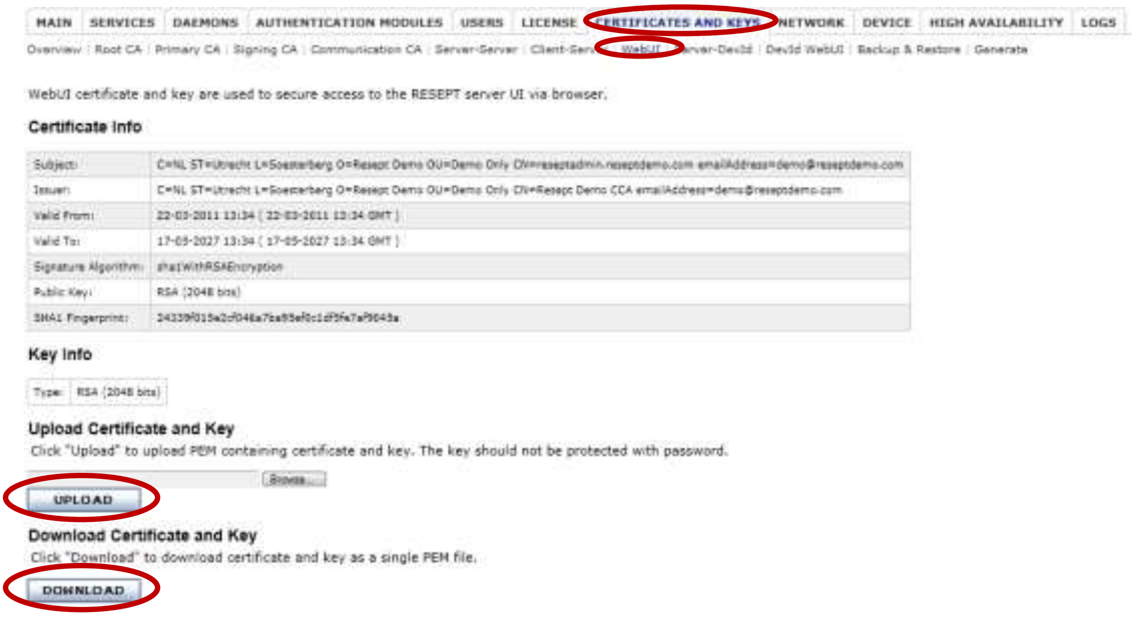
To make the changes permanent, please refer to section 8.2 ‘Saving changes & reboot’.

22.7. WebUI Certificate & Key

This tab allows you to view the information of the KeyTalk Admin Graphical User Interface.

It is used to secure the communication between the KeyTalk appliance and the computer of the organization’s administrator (single SSL). You should choose to purchase this certificate ad key from a 3rd party certificate provider. For more information please refer to section 8.1 ’Replacing Admin GUI SSL-certificate’.

A separate WebUI key and certificate are required for each KeyTalk and DevID appliance, since each appliance will run under its own unique FQDN in the network.


MAIN
SERVICES
DAEMONS
AUTHENTICATION MODULES
USERS
LICENSE
CERTIFICATES AND KEYS
NETWORK
DEVICE
HIGH AVAILABILITY
LOGS
Overview | Root CA | Primary CA | Signing CA | Communication CA | Server-Server | Client-Server | WebUI | Server-DevId | DevId WebUI | Backup & Restore | Generate
Browse...
UPLOAD
DOWNLOAD

WebUI certificate and key are used to secure access to the RESEPT server UI via browser.

Certificate Info

Subject:	C=NL ST=Utrecht L=Soesterberg O=Resept Demo OU=Demo Only CN=reseptadmin.reseptdemo.com emailAddress=demo@reseptdemo.com
Issuer:	C=NL ST=Utrecht L=Soesterberg O=Resept Demo OU=Demo Only CN=Resept Demo CCA emailAddress=demo@reseptdemo.com
Valid From:	22-03-2011 13:34 (22-03-2011 13:34 GMT)
Valid To:	17-05-2027 13:34 (17-05-2027 13:34 GMT)
Signature Algorithm:	sha1WithRSAEncryption
Public Key:	RSA (2048 bits)
SHA1 Fingerprint:	24339f015a2cf046a7ba95ef0c1df5fa7af9045a

Key Info

Type:	RSA (2048 bits)

Upload Certificate and Key

Click "Upload" to upload PEM containing certificate and key. The key should not be protected with password.

Download Certificate and Key

Click "Download" to download certificate and key as a single PEM file.

Figure 105: WebUI certificate information and key upload functionality

This screen allows you to download the current certificate and key, and upload a new version.

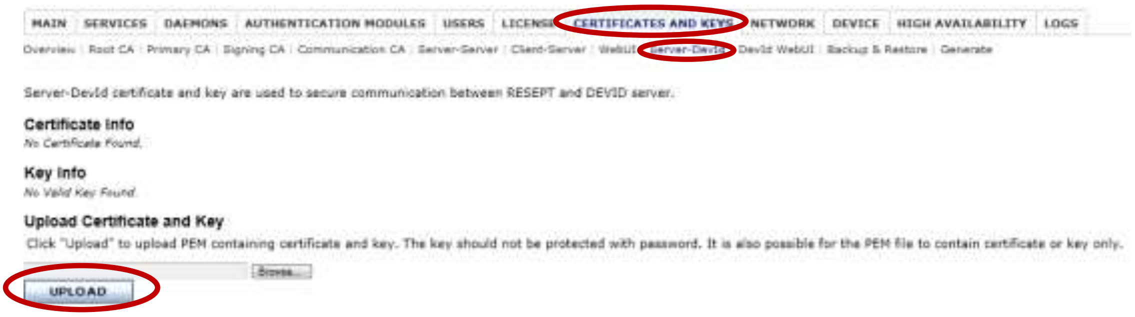
A new certificate can be uploaded by selecting it via “Browse…” and clicking “UPLOAD”.

After a successful UPLOAD the device management subsystem will automatically restart to effectuate the new certificate.

To make the changes permanent, please refer to section 8.2 ‘Saving changes & reboot’.

22.8. Server-DevID Certificate & Key

The Server-DevID certificate and key is used to secure communication between the KeyTalk Server and the DevID appliance.


MAIN
SERVICES
DAEMONS
AUTHENTICATION MODULES
USERS
LICENSE
CERTIFICATES AND KEYS
NETWORK
DEVICE
HIGH AVAILABILITY
LOGS
Overview | Root CA | Primary CA | Signing CA | Communication CA | Server-Server | Client-Server | WebUI | Server-DevId | DevId WebUI | Backup & Restore | Generate
Browse...
UPLOAD

Server-DevId certificate and key are used to secure communication between RESEPT and DEVID server.

Certificate Info

No Certificate Found.

Key Info

No Valid Key Found.

Upload Certificate and Key

Click "Upload" to upload PEM containing certificate and key. The key should not be protected with password. It is also possible for the PEM file to contain certificate or key only.

Figure 106: Server-DevID certificate information and key upload functionality

A new certificate can be uploaded by selecting it via “Browse…” and clicking “UPLOAD”.

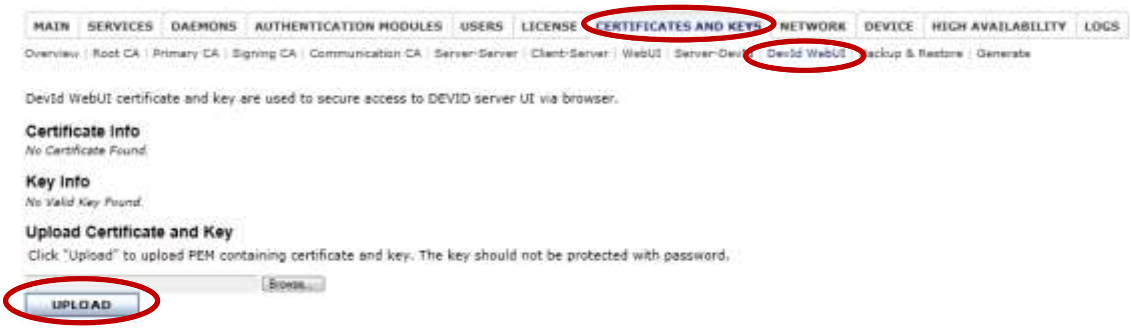
After a successful UPLOAD the device management subsystem will automatically restart to effectuate the new certificate.

To make the changes permanent, please refer to section 8.2 ‘Saving changes & reboot’.

22.9. DevID WebUI Certificate & Key

The DevID WebUI certificate and key are used to secure access to the DevID server UI via a browser.

A separate DevID WebUI key and certificate are required for each DevID appliance, since each one will run under its own unique FQDN in the network.


MAIN
SERVICES
DAEMONS
AUTHENTICATION MODULES
USERS
LICENSE
CERTIFICATES AND KEYS
NETWORK
DEVICE
HIGH AVAILABILITY
LOGS
Overview | Root CA | Primary CA | Signing CA | Communication CA | Server-Server | Client-Server | WebUI | Server-DevId | DevId WebUI | Backup & Restore | Generate

DevId WebUI certificate and key are used to secure access to DEVID server UI via browser.

Certificate Info
No Certificate Found.

Key Info
No Valid Key Found.

Upload Certificate and Key
Click "Upload" to upload PEM containing certificate and key. The key should not be protected with password.

Figure 107: DevID WebUI certificate information and key upload functionality

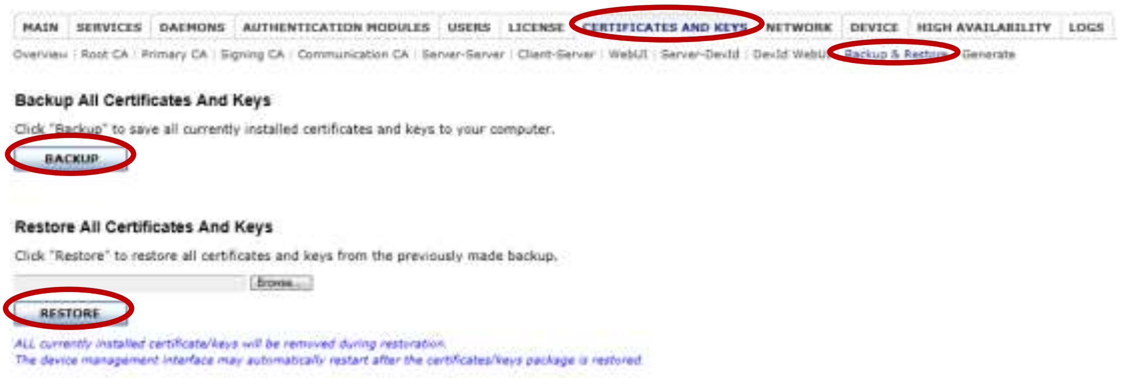
A new certificate can be uploaded by selecting it via “Browse…” and clicking “UPLOAD”.

After a successful UPLOAD the device management subsystem will automatically restart to effectuate the new certificate.

To make the changes permanent, please refer to section 8.2 ‘Saving changes & reboot’.

22.10. Backup & Restore

This tab allows you to make a full backup of your current certificates and keys, as well as granting the ability to restore your backup, if required.


MAIN
SERVICES
DAEMONS
AUTHENTICATION MODULES
USERS
LICENSE
CERTIFICATES AND KEYS
NETWORK
DEVICE
HIGH AVAILABILITY
LOGS
Overview | Root CA | Primary CA | Signing CA | Communication CA | Server-Server | Client-Server | WebUI | Server-DevId | DevId WebUI | Backup & Restore | Generate
BACKUP
Browse...
RESTORE

Backup All Certificates And Keys

Click "Backup" to save all currently installed certificates and keys to your computer.

Restore All Certificates And Keys

Click "Restore" to restore all certificates and keys from the previously made backup.

ALL currently installed certificate/keys will be removed during restoration.
The device management interface may automatically restart after the certificates/keys package is restored.

Figure 108: Backup and restore functionality

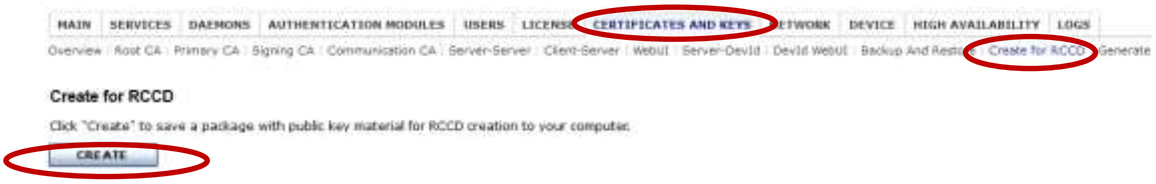
Click "Backup" to save all currently installed certificates and keys to your computer.

Click "Restore" to restore all certificates and keys from the previously made backup. The KeyTalk appliance will reboot afterwards, to effectuate the changes.

22.11. Create for RCCD

This tab allows you to download all PUBLIC material required to create your own RCCD files for your organization within the KeyTalk signingportal. To access the KeyTalk signing portal you are required to either be a KeyTalk partner serving at least 1 active customer, or be an active customer.

Potential customers who are playing with the free trial software under the demo license may contact KeyTalk support or a relevant KeyTalk partner to enter into an agreement free of charge to use KeyTalk using unique Key Material for Proof of Concept purposes for an agreed amount of time.


MAIN
SERVICES
DAEMONS
AUTHENTICATION MODULES
USERS
LICENSE
CERTIFICATES AND KEYS
NETWORK
DEVICE
HIGH AVAILABILITY
LOGS
Overview | Root CA | Primary CA | Signing CA | Communication CA | Server-Server | Client-Server | WebUI | Server-DevId | DevId WebUI | Backup And Restore | Create for RCCD | Generate
CREATE

Create for RCCD

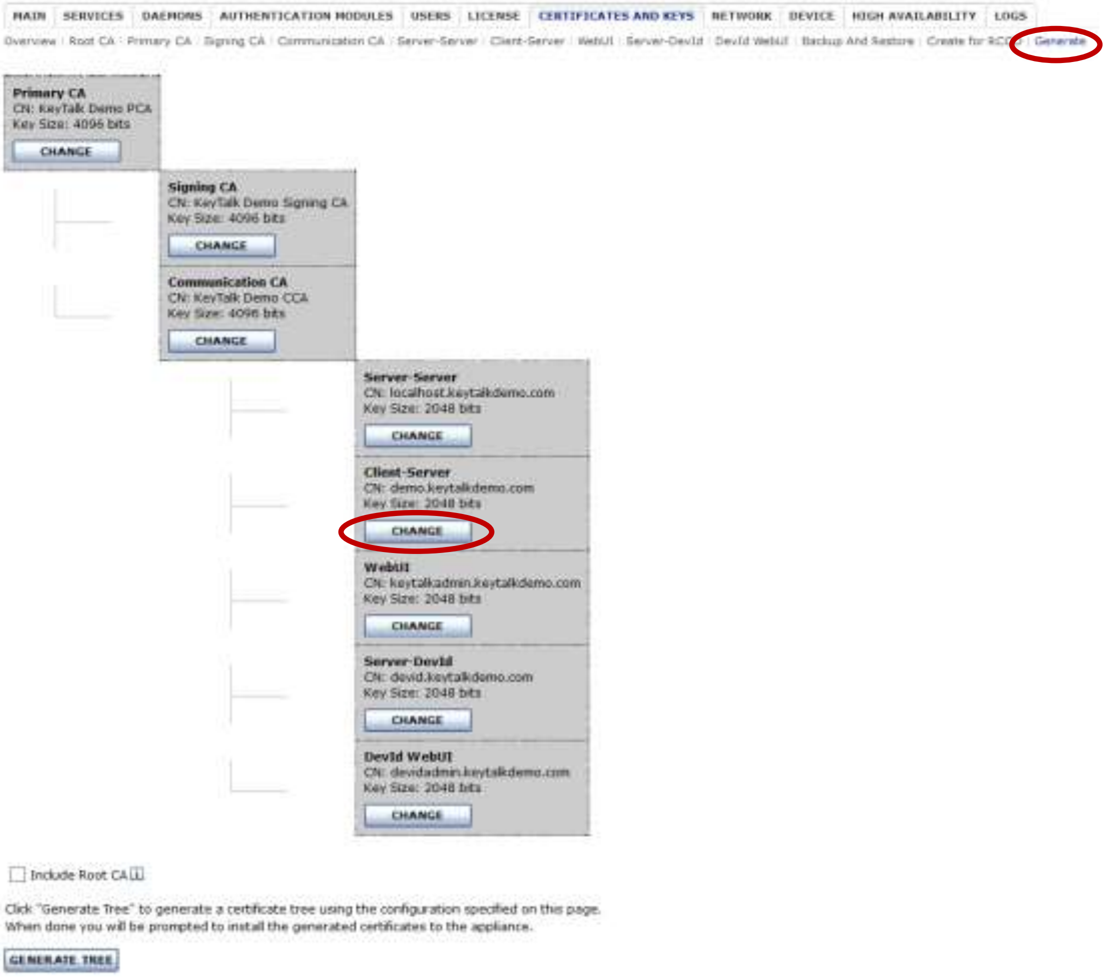
Click "Create" to save a package with public key material for RCCD creation to your computer.

22.12. Generate

This tab allows you to edit specific criteria for the certificates that have been generated on the appliance.

Always ensure your <u>parent certificate</u> has <u>the same or higher values</u> than its child, ref the signature algorithm, the lifetime and the key-size

The Signing CA signs the client certificates that get issues. When you choose SHA256 also your client certificates will make use of SHA256 hashing.


MAIN
SERVICES
DAEMONS
AUTHENTICATION MODULES
USERS
LICENSE
CERTIFICATES AND KEYS
NETWORK
DEVICE
HIGH AVAILABILITY
LOGS
Overview | Root CA | Primary CA | Signing CA | Communication CA | Server-Server | Client-Server | WebUI | Server-DevId | DevId WebUI | Backup And Restore | Create for RCCD | Generate
CHANGE
GENERATE TREE

Primary CA
CN: KeyTalk Demo PCA
Key Size: 4096 bits

Signing CA
CN: KeyTalk Demo Signing CA
Key Size: 4096 bits

Communication CA
CN: KeyTalk Demo CCA
Key Size: 4096 bits

Server-Server
CN: localhost.keytalkdemo.com
Key Size: 2048 bits

Client-Server
CN: demo.keytalkdemo.com
Key Size: 2048 bits

WebUI
CN: keytalkadmin.keytalkdemo.com
Key Size: 2048 bits

Server-DevId
CN: devid.keytalkdemo.com
Key Size: 2048 bits

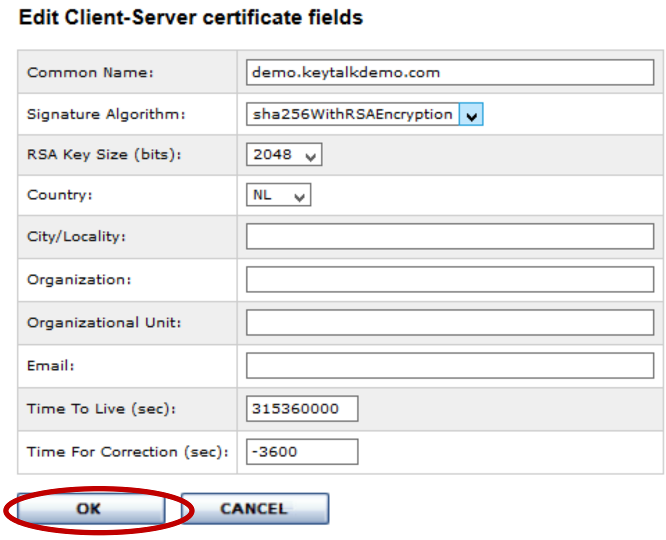
DevId WebUI
CN: devidadmin.keytalkdemo.com
Key Size: 2048 bits

□ Include Root CA

Click "Generate Tree" to generate a certificate tree using the configuration specified on this page. When done you will be prompted to install the generated certificates to the appliance.

Figure 109: Edit specific criteria for all hosted certificates

Click on 'CHANGE' to edit a specific set of certificate fields. Click 'OK' to accept the alterations.

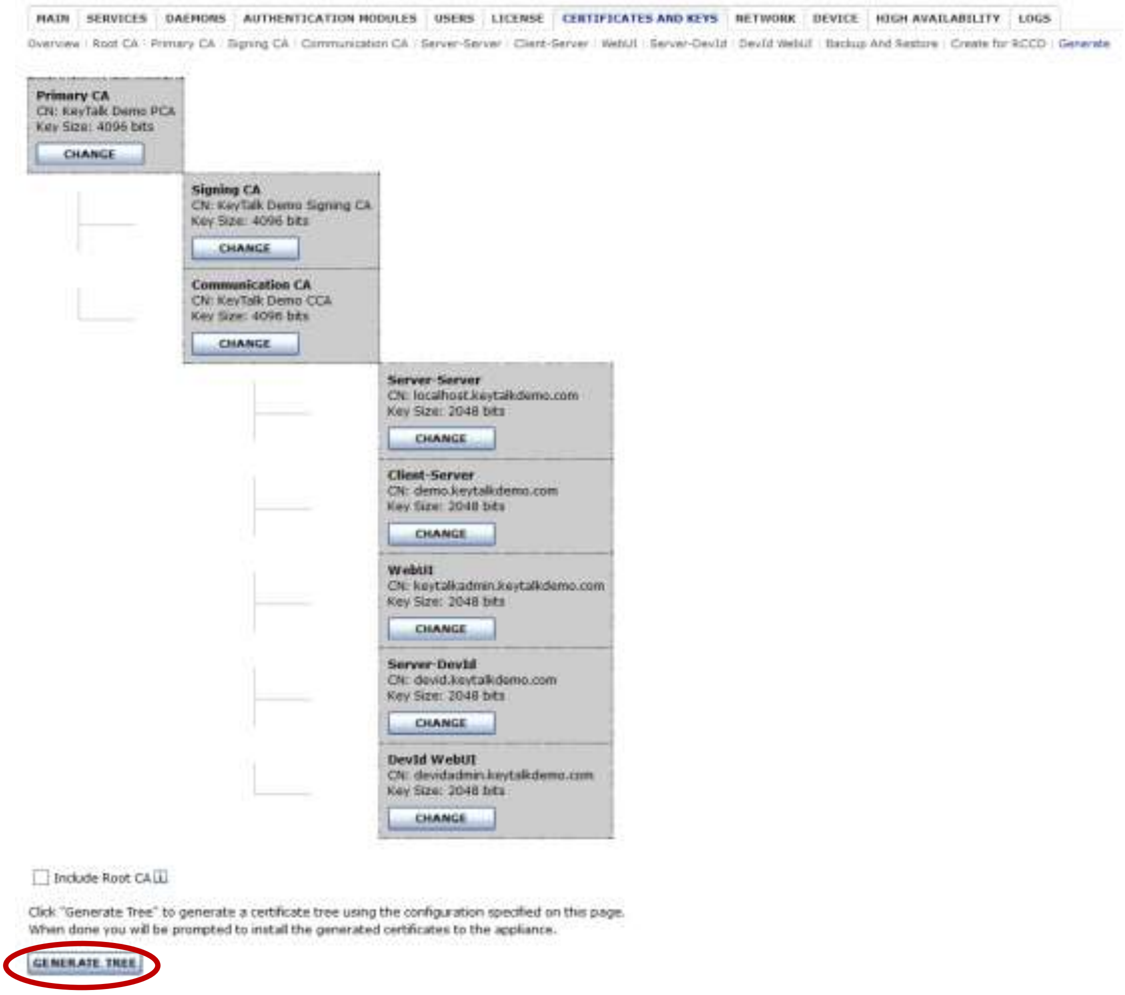


Edit Client-Server certificate fields

Common Name:	demo.keytalkdemo.com
Signature Algorithm:	sha256WithRSAEncryption
RSA Key Size (bits):	2048
Country:	NL
City/Locality:	
Organization:	
Organizational Unit:	
Email:	
Time To Live (sec):	315360000
Time For Correction (sec):	-3600

Figure 110: Edit specific Client-Server certificate fields

Once you have finished editing the necessary certificate fields; you are ready to generate the newly configured certificate tree.


MAIN
SERVICES
DAEMONS
AUTHENTICATION MODULES
USERS
LICENSE
CERTIFICATES AND KEYS
NETWORK
DEVICE
HIGH AVAILABILITY
LOGS
Overview | Root CA | Primary CA | Signing CA | Communication CA | Server-Server | Client-Server | WebUI | Server-DevId | DevId WebUI | Backup And Restore | Create for RCCD | Generate
CHANGE
GENERATE TREE

Primary CA
CN: KeyTalk Demo PCA
Key Size: 4096 bits

Signing CA
CN: KeyTalk Demo Signing CA
Key Size: 4096 bits

Communication CA
CN: KeyTalk Demo CCA
Key Size: 4096 bits

Server-Server
CN: localhost.keytalkdemo.com
Key Size: 2048 bits

Client-Server
CN: demo.keytalkdemo.com
Key Size: 2048 bits

WebUI
CN: keytalkadmin.keytalkdemo.com
Key Size: 2048 bits

Server-DevId
CN: devid.keytalkdemo.com
Key Size: 2048 bits

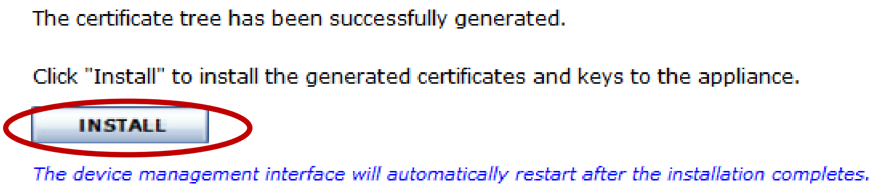
DevId WebUI
CN: devidadmin.keytalkdemo.com
Key Size: 2048 bits

☐ Include Root CA

Click "Generate Tree" to generate a certificate tree using the configuration specified on this page. When done you will be prompted to install the generated certificates to the appliance.

Figure 111: Generate the newly configured tree

Click "Generate Tree" to generate a certificate tree using the configuration specified on this page. When done you will be prompted to install the generated certificates to the appliance.



The certificate tree has been successfully generated.

Click "Install" to install the generated certificates and keys to the appliance.

The device management interface will automatically restart after the installation completes.

Figure 112: Install the generated certificate tree

After a successful UPLOAD the device management subsystem will automatically restart to effectuate the new certificate tree. If for whatever reason it doesn't please do so manually.

To make the changes permanent, please refer to section 8.2 '<u>Saving changes & reboot</u>'.

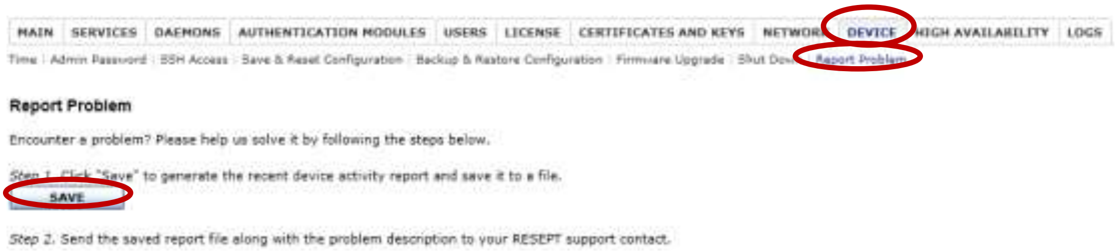
23. Errors and error-reporting

When KeyTalk server encounters an error, KeyTalk Client displays an appropriate error message. The most typical server-side errors are- Resolved IP invalid

- Digest Invalid

- Time out of sync

When server error cannot be resolved, the Admin should run “Report Problem” function.


MAIN
SERVICES
DAEMONS
AUTHENTICATION MODULES
USERS
LICENSE
CERTIFICATES AND KEYS
NETWORK
DEVICE
HIGH AVAILABILITY
LOGS
Time | Admin Password | SSH Access | Save & Reset Configuration | Backup & Restore Configuration | Firmware Upgrade | Shut Down | Report Problem
SAVE

Report Problem

Encounter a problem? Please help us solve it by following the steps below.

Step 1. Click "Save" to generate the recent device activity report and save it to a file.

Step 2. Send the saved report file along with the problem description to your RESEPT support contact.

Figure 113: Generate a problem activity report

Save the resulting file, and send it to your KeyTalk supplier or partner with a written description of the problem, preferably substantiated with screenshots, repro steps and log files. Please make sure to always have a generated problem report before contacting support to assist fast troubleshooting.

24. LCD information display

Does not apply to the virtual appliance.

Front Panel component ‘J’ provides information to those accessing the physical KeyTalk appliance.

Using buttons A, B, C and D, allows you to navigate the different information screens on the LED display.

Normal mode				
Button	A	B	C	D
Effect	Back	Up	Down	Confirm

Direct code mode				
Button	A	B	C	D
Effect	Position 1: 0-9	Position 2: 0-9	Position 3: 0-9	Confirm

To activate the LCD information display menu, touch any of the buttons A, B, C or D.

After it has been activated you can press ‘D’ to activate the Direct Code mode. Press buttons A-C to go to the Normal mode.

Select and confirm any of the three figure menu items will make the LCD go to its default display.

Menu item			**Description**	**Effect**
		Direct code		
0			Direct code	Activate direct code
1			Device	Go to device sub-menu
	11		Power	Go to the power sub-menu
		111	Reboot	Reboot the appliance. This will make the active configurations persistent.
	12		IP reset	Go to IP reset sub-menu
		121	External	Reset the external IP to default (perform 131 manually)
		122	Internal	Reset the internal IP to default (perform 131 manually)
		123	Management	Reset the management IP to default (perform 131 manually)
	13		Maintenance	Go to the KeyTalk maintenance sub-menu
		131	Reset users	Reset the oldest 10% of the user license count
		132	Save Settings	Save changed settings
		133	Reset Settings	Reset all appliance settings to factory default and reboot
		134	Upgrade	Activate the FWUPGRADE
2			Info	Go to the information sub-menu
	21		KeyTalk	Go to the KeyTalk information sub-menu
		211	Version	Display the current KeyTalk appliance firmware version
		212	Counted users	Display counted users for license purposes

	22		IP Address	Go to the IP information sub-menu
		221	External	Display the current external IP number
		222	Internal	Display the current internal IP number
		223	Management	Display the current management IP number

25. Release notes

25.1. KeyTalk Appliance firmware

Version	Release date	Description
4.0.0	June 1st 2011	Initial release
4.1	January 23rd 2012	Significant efficiency improvement, upgraded OS, upload firmware option, added DevID module support, updated HAD functionality, download & remove functions on daemon certificates & keys, total unique users per service reporting, LCD based oldest unique user cleaning (max 10%)
4.2	July 2012	Update documentation to KeyTalk 4.2. In 4.2 it is possible to generate the CA tree on the appliance.
4.3	October 2013	- ADDED full RADIUS authentication - ADDED RADIUS field name change option on authentication type for client purposes - ADDED Active Directory Service Account for password change after password expired from client - ADDED Windows BIOS DevID option - ADDED RCCD certificate files download button
4.3.3	March 2014	- Updated core engine - Added SHA256 to CA-tree generation - Improved LDAP BIND options - Allow for “no empty password” for LDAP/AD - Improved RADIUS to support RSA SecurID - For the minor details please visit our website: http://www.keytalk.com/downloads/KeyTalkApplianceReleaseNotes.txt

26. Manufacturer information

Manufacturer: KeyTalk 1 BV
Nijverheidsweg Noord 78
3812 PM Amersfoort
The Netherlands

Telephone: +31 (0)88 KEYTALK
Email: info@keytalk.com
Web: www.keytalk.com

Chamber of Commerce: 59072555
VAT Number: NL853305766B01

Bank: Rabobank

Bank	NL78 RABO 0133 2932 38
BIC	RABONL2U