



HSA User Manual

HSA V050, 14. September 2018

Index

1	HSA Quick Start Guide	6
1.1	LEDs and buttons.	6
1.2	How to power on.	7
1.3	How to access the HSA.....	7
1.4	How to completely power off (for storage or shipping).	7
1.5	Recommended PuTTY settings.....	8
1.6	Manual Download.....	8
2	Setup Wizard	10
2.1	Starting the Wizard	10
2.2	Changing IP.....	10
2.2.1	Select Interface.....	11
2.2.2	Enter IP	11
2.2.3	Gateway	12
2.2.4	Confirm settings and reconnect.....	12
2.3	Changing DNS.....	12
2.4	Setting the correct time	13
2.4.1	Setting timezone	13
2.4.2	Enter date.....	14
2.4.3	Enter time.....	14
2.5	Changing NTP	15
2.6	Changing password.....	15
2.7	Setup of a new YubiHSM.....	15
2.7.1	Creating a wrapping key.....	15
2.7.2	Creating the admin authentication key.....	16
2.8	Creating a PKI authentication key.....	18
2.8.1	Authentication key ID.....	19
2.8.2	Authentication key label	20
2.8.3	Authentication key domain.....	20
2.8.4	Choose a password.....	21

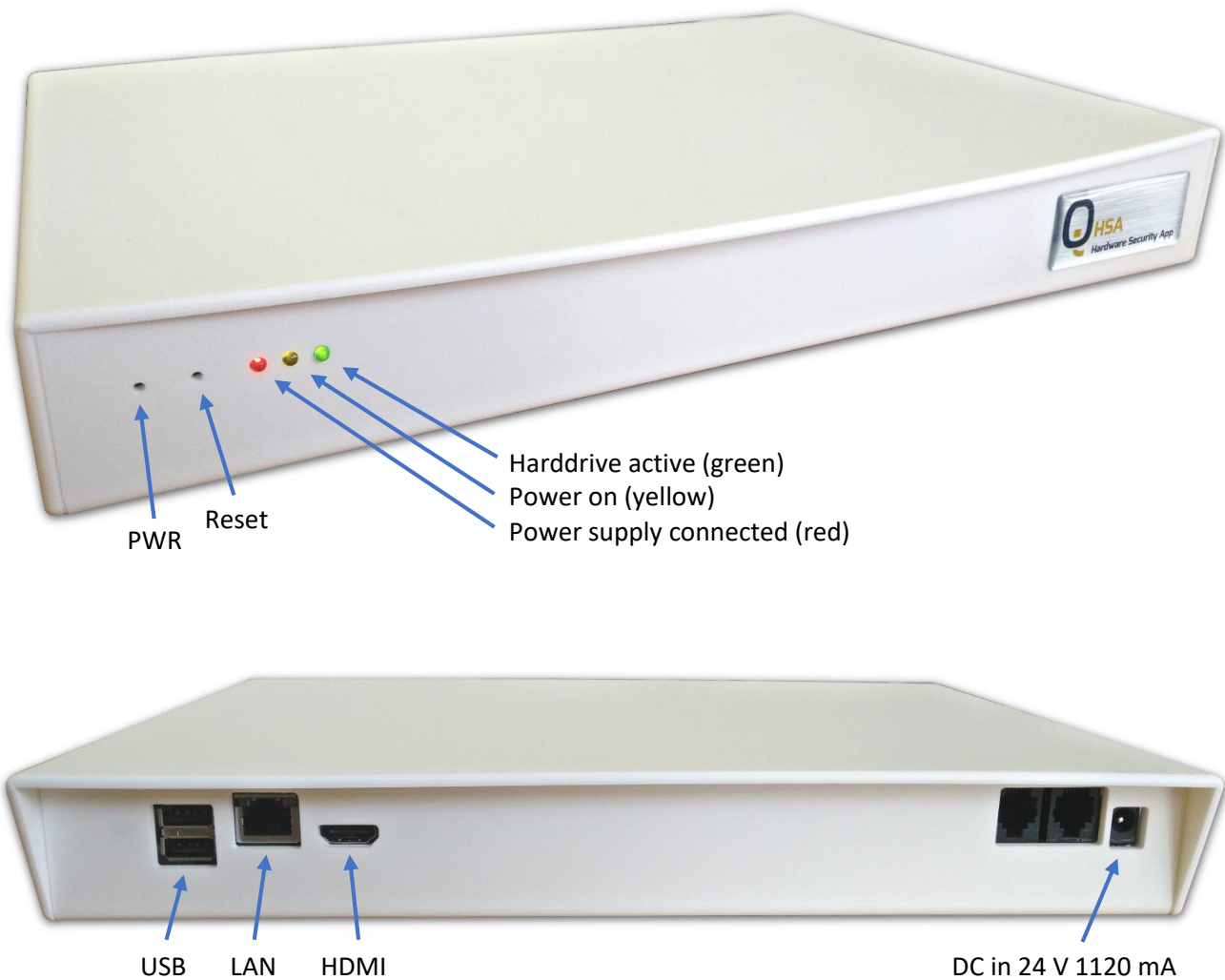
2.8.5	PKI authentication key stored on the YubiHSM	21
2.9	Creating a new connector certificate	21
2.10	Wizard completed	23
3	The main menu	24
4	The network menu	25
4.1	hostname	25
4.2	interface	25
4.2.1	Edit interface	26
4.3	DNS	26
4.4	addRoute	26
4.5	listRoute	26
4.6	NTP	26
5	The yubiHSM menu	27
5.1	info	27
5.2	setup	27
5.3	authkey	27
5.4	backup	27
5.5	readBackup	27
5.6	shell	28
5.7	deviceinfo	28
5.8	connector	28
5.8.1	restartCon	28
5.8.2	rmSN	28
5.8.3	writeSN	28
5.8.4	manSN	29
5.8.5	restartNginx	29
5.8.6	cert	29
5.8.7	allowIP	29
5.8.8	listIP	29
6	The HSA menu	29

6.1	users	30
6.2	time	30
6.3	update	30
6.4	backup	30
6.5	restore	30
6.6	wizard	31
6.7	LinuxCLI	31
6.8	reboot	31
6.9	shutdown	31
7	The logging menu	31
7.1	Syslog	31
7.1.1	local	32
7.1.2	remote	32
7.1.3	server	32
7.1.4	TLS	32
7.1.5	filter	32
7.2	SNMP	34
7.2.1	enable/disable	34
7.2.2	OID	34
7.2.3	port	34
7.2.4	sysLocation	34
7.2.5	sysContact	34
7.2.6	user	34
7.2.7	listUser	35
8	YubiHSM setup on a PKI Server	36
8.1	Installing the connector certificate	36
8.2	Installing the YubiHSM Key Storage Prvider.	37
8.3	Add the CA Role	39
8.4	Configure Active Directory Certificate Services	41
9	Troubleshooting	46

9.1 Active Directory Certificate Services.....	46
--	----

1 HSA Quick Start Guide

1.1 LEDs and buttons.



1.2 How to power on.

Plug in the power supply and the HSA will start automatically (indicated by power on LED).
If the red LED is on but the yellow LED not, you can press the PWR button to power on.

Please do not connect the HSA to your network before changing the IP address.

1.3 How to access the HSA

You can connect to the HSA box via SSH using PuTTY or another SSH client.
Or with an HDMI monitor and a USB keyboard.

Default IP/Netmask: 192.168.0.1/24
Default Gateway: 192.168.0.254
Default DNS: 192.168.0.254

Default user and password:
deviceadmin

When you log in for the first time, the Setup Wizard starts, and you can specify the most important settings.

More detailed setup information can be found in the “HSA Setup Manual”, which you can download directly from the HSA as described in Manual Download on the next page.

1.4 How to completely power off (for storage or shipping).

The HSA is equipped with a battery.

If you want to ship the device or store it for a longer period of time, please follow these steps to completely power off.

In the menu

Go to The HSA menu > shutdown

On the CLI

Enter: sudo shutdown now

Or press the PWR button.

After the yellow LED turns off, unplug the power supply and press the Reset button for 5 seconds.

If everything is completely powered off, the PWR button doesn't work and you should only be able to power on the HSA by plugging in the power supply.

1.5 Recommended PuTTY settings

By default, the numeric keypad does not enter numbers in the HSA menu, but is used as the directional keys when using PuTTY.

To change that, do the following:

Open PuTTY and click on “Terminal” > “Functions”.
Enable “Disable application keypad mode”.

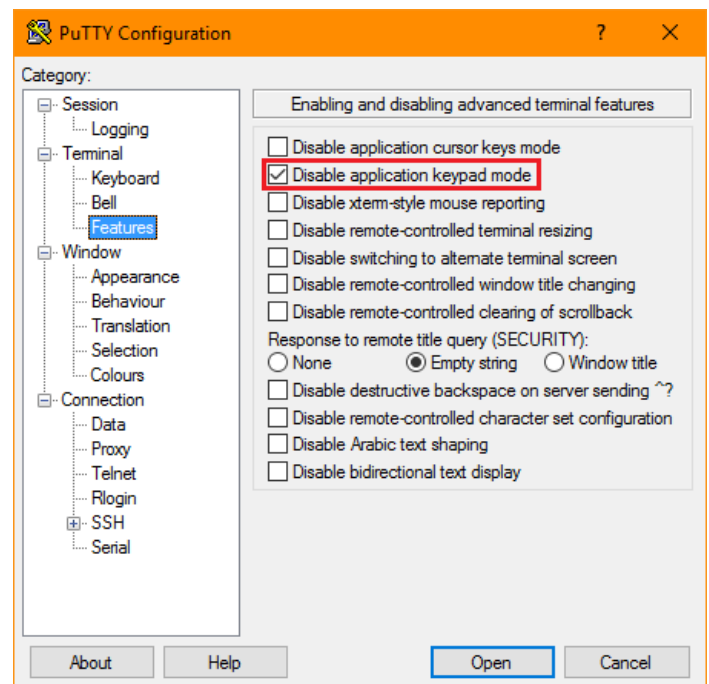
It is also recommended to change the window and text size for readability.

“Window” - “Columns” and “Rows”

“Window” > “Appearance” - “Font Settings”

The font “Consolas” works very well for terminals.

To save this as the default settings click on
“Session”, in the “Saved Sessions” textfield enter
“Default Settings” and click “Save”.



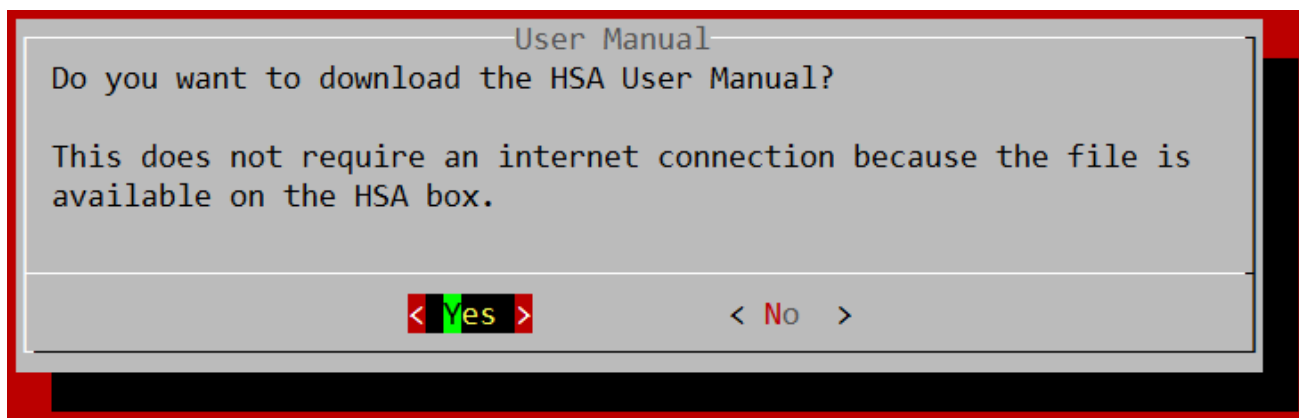
1.6 Manual Download

The Quick Start Guide is included in printed form in the HSA package.

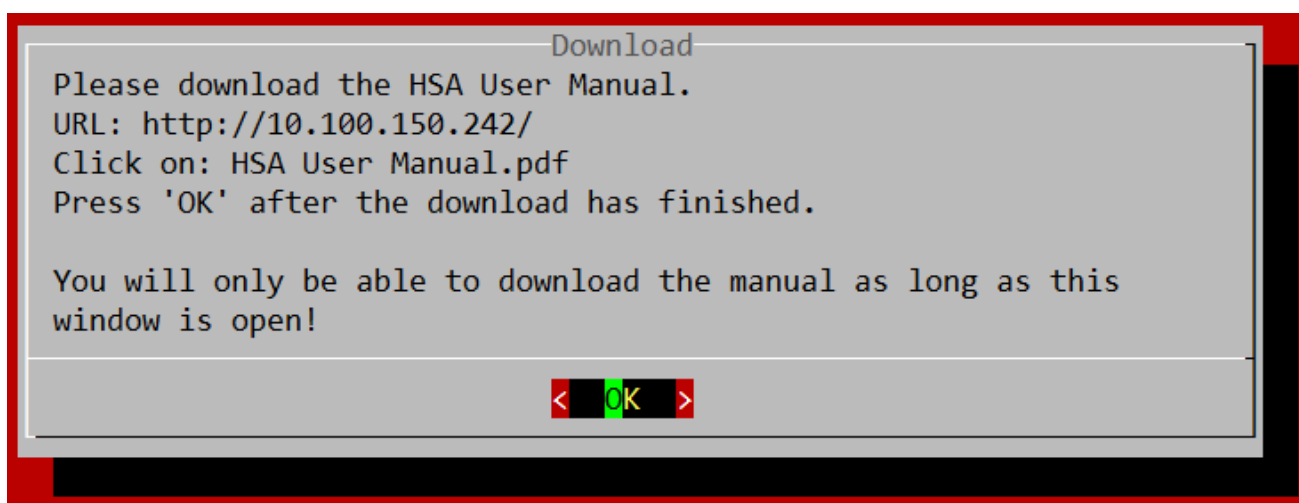
The more detailed manual is only available as PDF.

You can download it directly from the HSA as follows. After the first login the wizard starts, select “Yes”.





The wizard asks if you want to download the HSA User Manual. Select “Yes”.



Open a web browser and enter the IP of your HSA (displayed in the “Download” window) in the address bar. Right click on “HSA User Manual.pdf” and select “Save target as ...”.

After downloading, make sure that you can open and read the HSA User Manual and click “OK”.

Alternatively, you can download the HSA User Manual online via FTP:
<ftp://customer:FZig9k@ftp2.iqsol.biz/6-IQSol-Customer/HSA/>



The HSA Quick Start Guide ends here.

Follow the instructions in Setup Wizard in the HSA User Manual PDF you just downloaded to continue setting up the HSA.

2 Setup Wizard

Please read the “HSA Quick Start Guide” before starting with the Setup Wizard.

2.1 Starting the Wizard



When you log on to the HSA for the first time, the setup wizard will start and guide you through the most important settings.

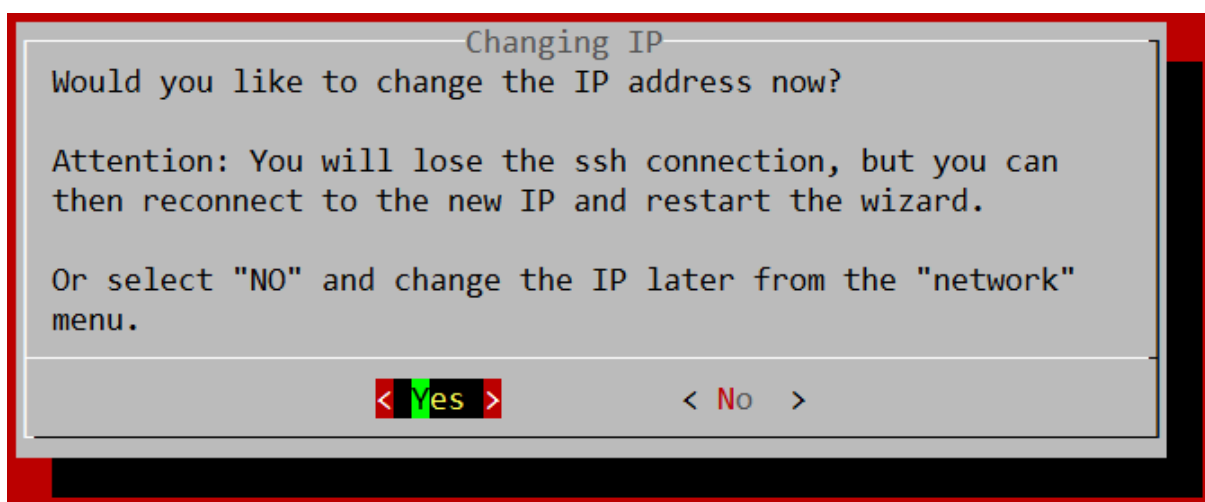
Select “Yes” to start the wizard or “No” if you already know all the important steps and want to select them manually in the menu.

This guide assumes that you are using the wizard.

2.2 Changing IP

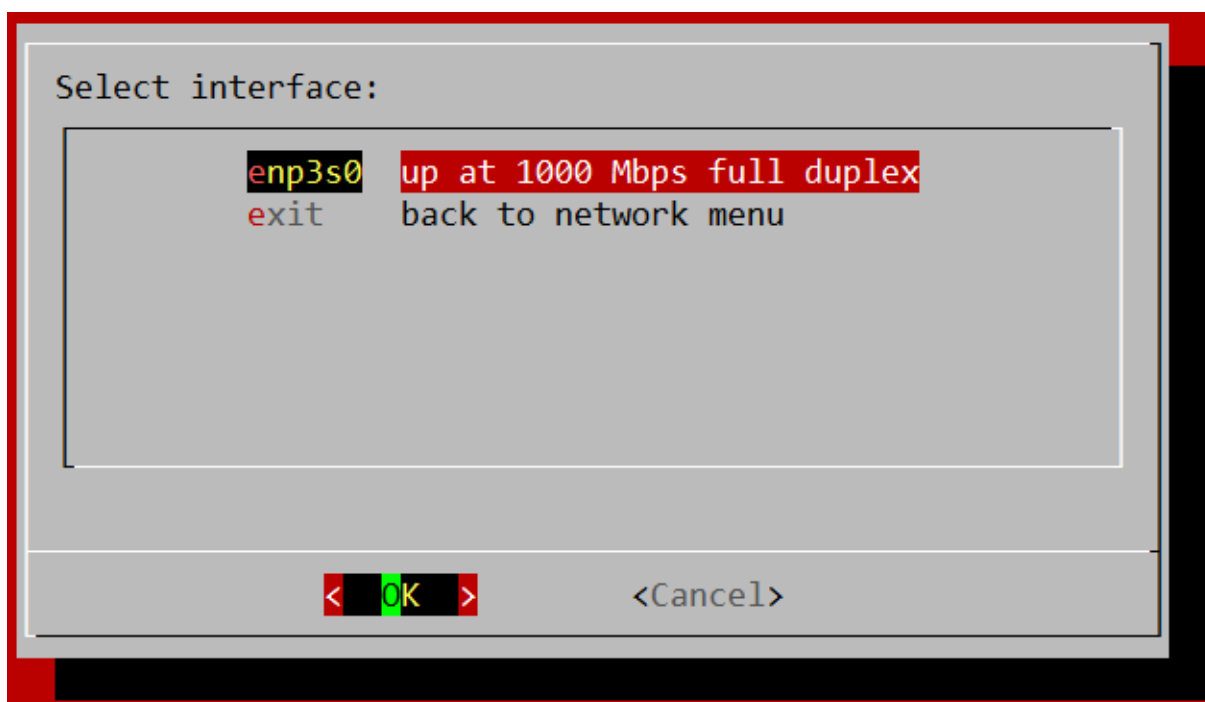
First you will be asked if you want to change the IP.

You can do this now and then log in to the new IP address to proceed with the wizard, or select “No” to change the IP address at the end in the menu, after everything else has been configured.



This guide assumes that you have selected “Yes”.

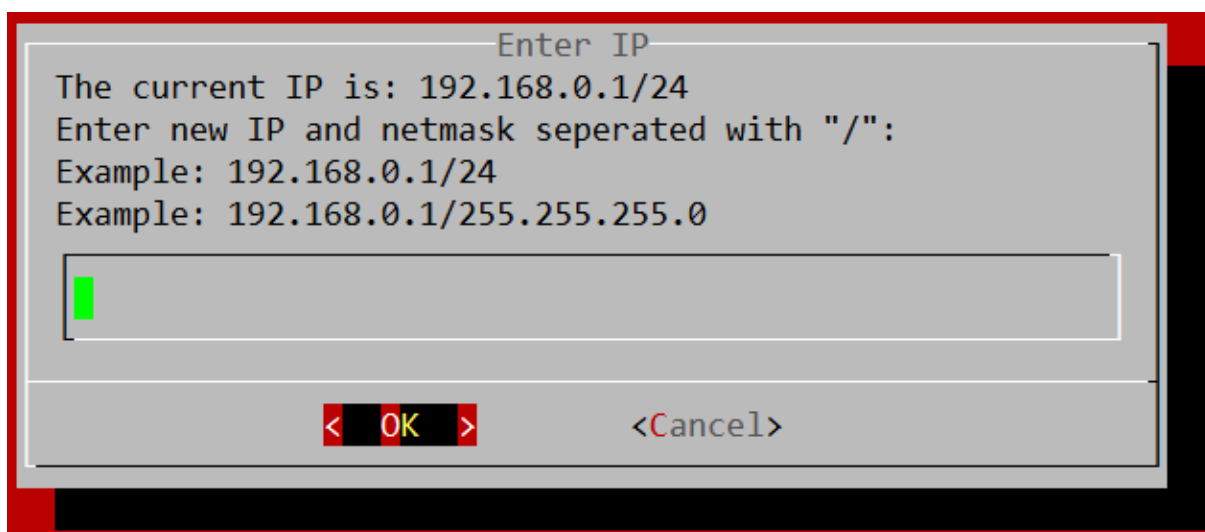
2.2.1 Select Interface



Now select the network interface on which you want to make changes.

On a standard HSA, only one should be present, just press “OK”.

2.2.2 Enter IP



Enter the new IP followed by the subnet mask like shown above.

You can enter the subnet mask as Classless Inter-Domain Routing (CIDR) suffix (example: 24) or dotted decimal notation (example: 255.255.255.0).

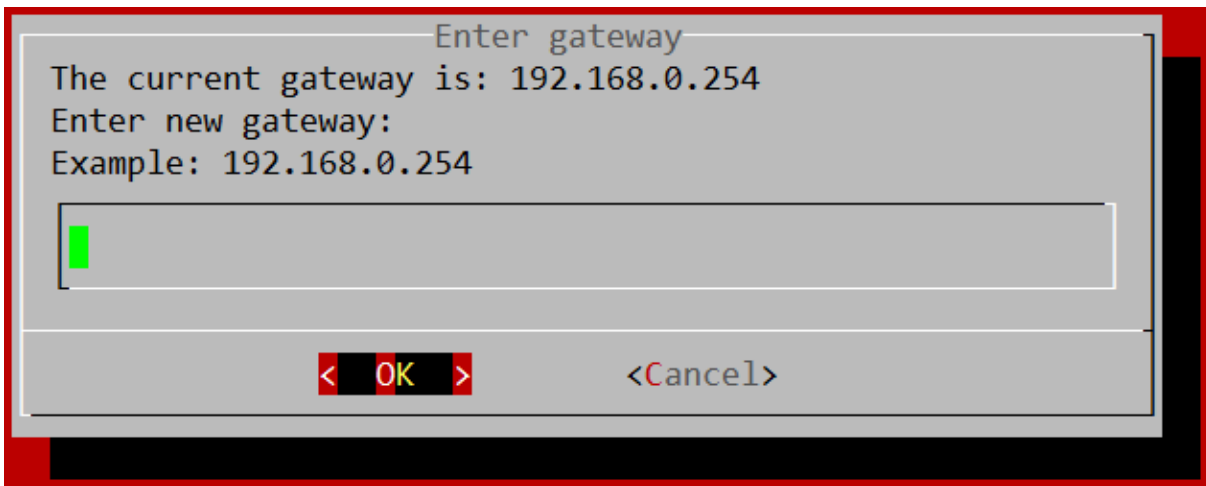
More info about this:

https://en.wikipedia.org/wiki/Classless_Inter-Domain_Routing

https://en.wikipedia.org/wiki/Dot-decimal_notation

2.2.3 Gateway

In the next step you will be asked to enter your gateway IP.



Click "OK". The settings will now be displayed again for confirmation.

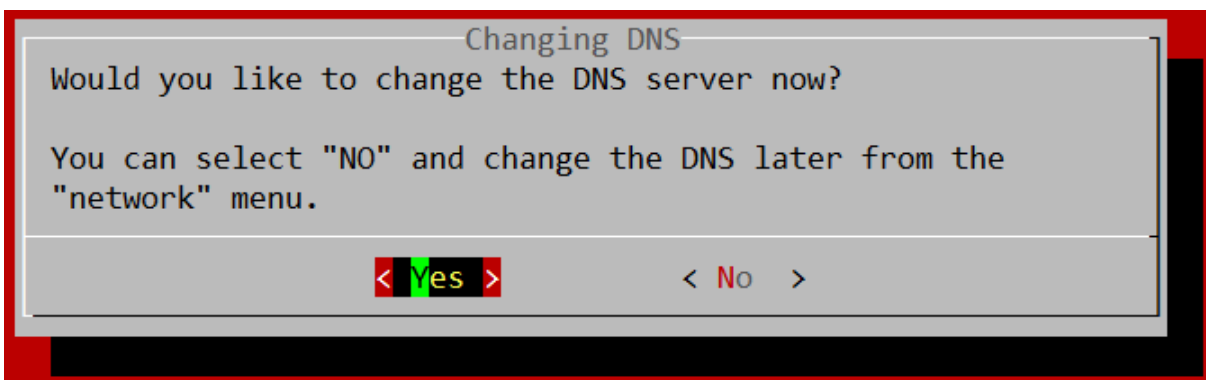
2.2.4 Confirm settings and reconnect

If everything looks fine select "Yes". If you are connected using SSH you will per design lose your connection. Now you can open a new SSH session to the new IP and proceed the wizard.

After logging in again and getting " Would you like to start the setup wizard now?" displayed, select "Yes".

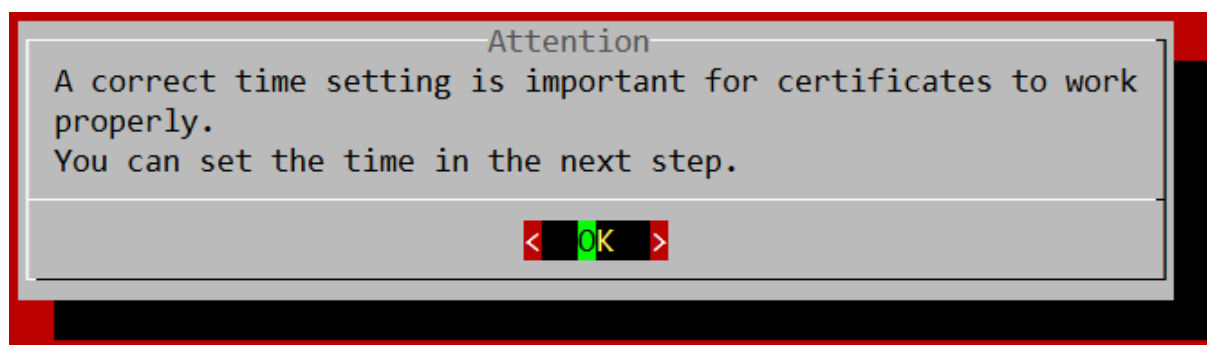
The wizard won't ask again if you want to change the IP, but will continue to the next step.

2.3 Changing DNS



Select "Yes" if you want to use a specific DNS Server and proceed with the wizard.

2.4 Setting the correct time



2.4.1 Setting timezone

```
Please identify a location so that time zone rules can be set correctly.
Please select a continent, ocean, "coord", or "TZ".
1) Africa
2) Americas
3) Antarctica
4) Asia
5) Atlantic Ocean
6) Australia
7) Europe
8) Indian Ocean
9) Pacific Ocean
10) coord - I want to use geographical coordinates.
11) TZ - I want to specify the time zone using the Posix TZ format.
#? █
```

Enter the number of your location and hit Enter.

For example, if you want to set "Europe/Vienna" as your time zone, input 7 and 4 in country selectin which is appearing after selecting a continent.

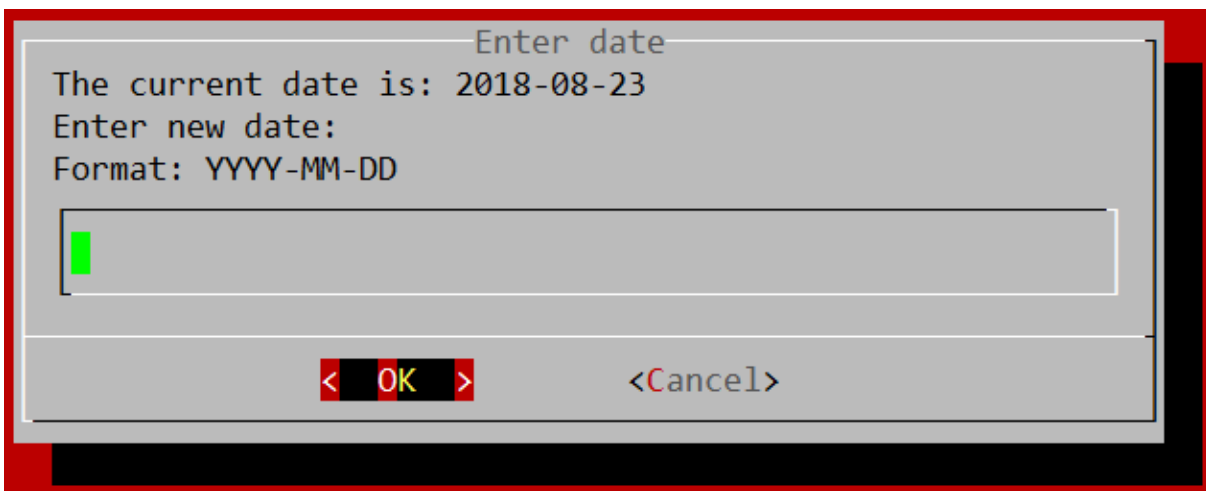
```
The following information has been given:

    Austria

Therefore TZ='Europe/Vienna' will be used.
Local time is now:      Thu Aug 23 10:52:07 CEST 2018.
Universal Time is now:  Thu Aug 23 08:52:07 UTC 2018.
Is the above information OK?
1) Yes
2) No
#? █
```

Confirm the settings by entering 1.

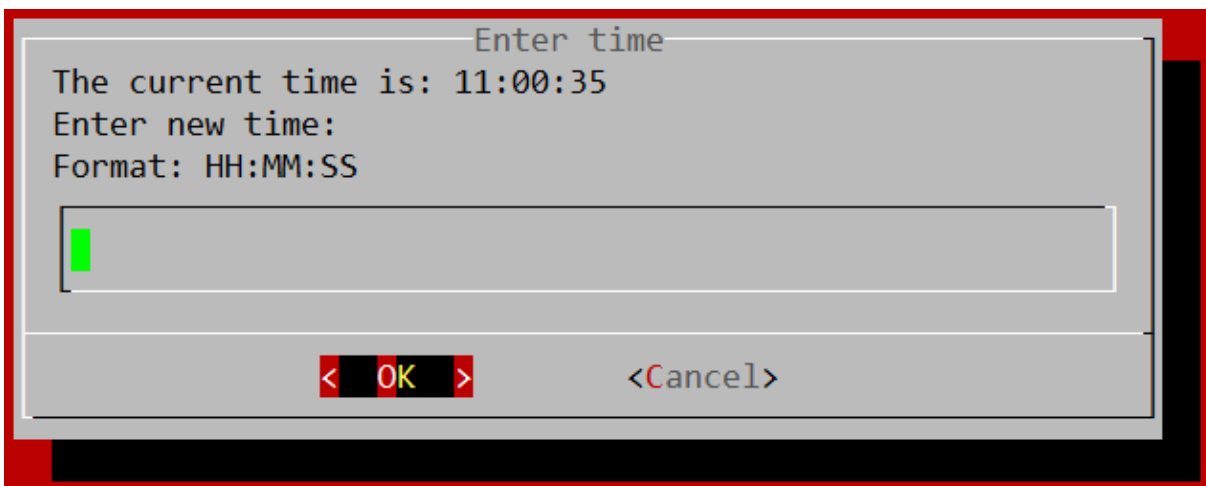
2.4.2 Enter date



Now enter the current date or just select “Cancel” if it is already correct.

If you selected “Cancel” you will be asked “No valid date was entered. Retry?” Select “No”.

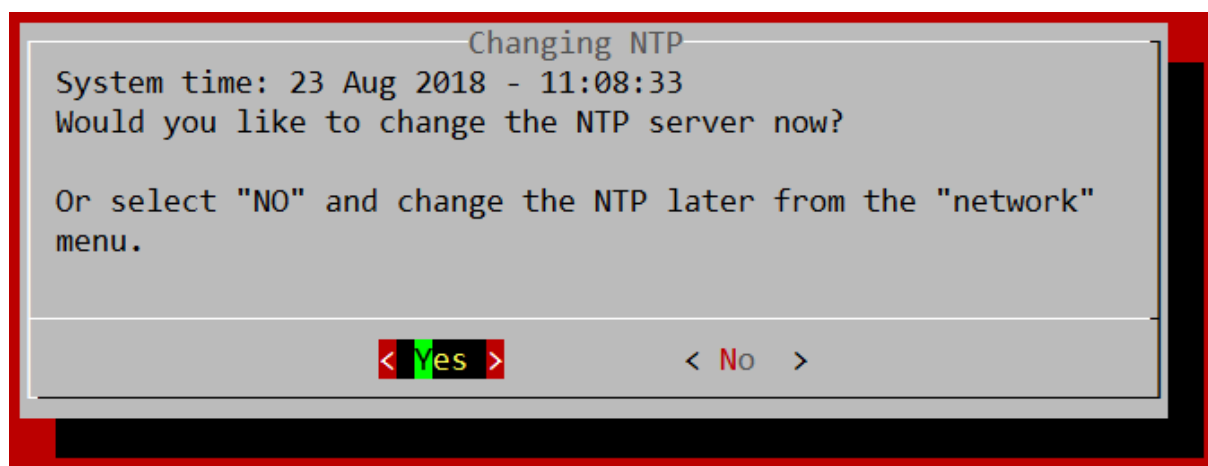
2.4.3 Enter time



Same as with date. You can select “Cancel” if the time is already correct.

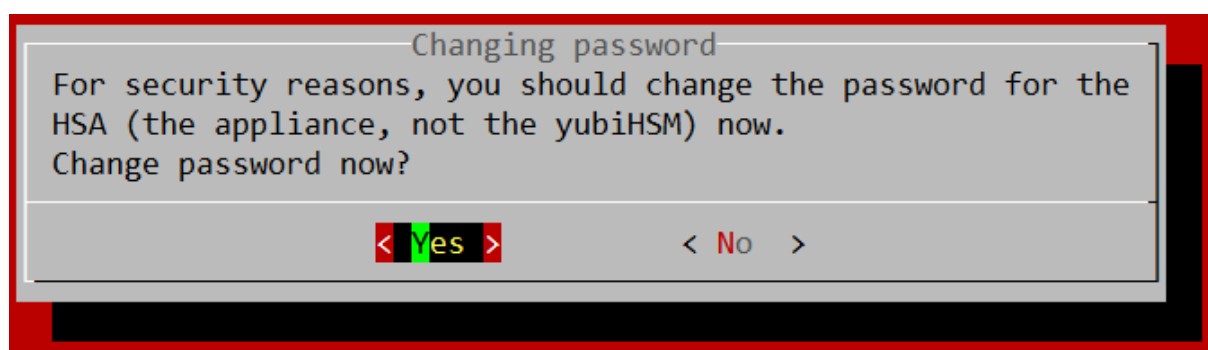
Note: The time in this screen is not updated live, but stays as it was when the screen first appeared. Time is still running in the background and will continue to do so if you choose Cancel.

2.5 Changing NTP



If you want to use a specific NTP server, select “Yes” and continue with the wizard.

2.6 Changing password



This is important for the HSA to be secure. Choose a secure password!

First for the default user “deviceadmin”, this user will mainly be used to configure the HSA.

The default password is: deviceadmin

Next you will be asked to change the root password. The root user will rarely be used and is only needed for some updates. This user should have a very strong password as it is allowed to do anything on the HSA.

The default password is: deviceadmin

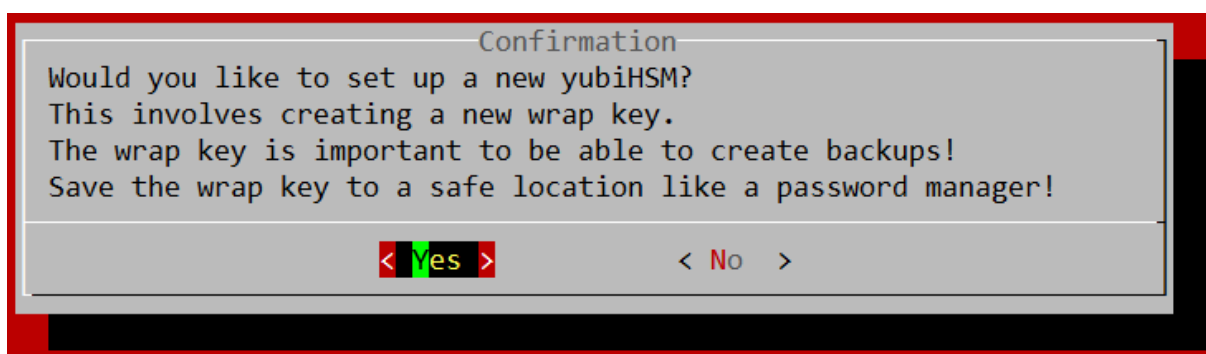
Note: The YubiHSM module has its own passwords and is not affected by these settings.

2.7 Setup of a new YubiHSM

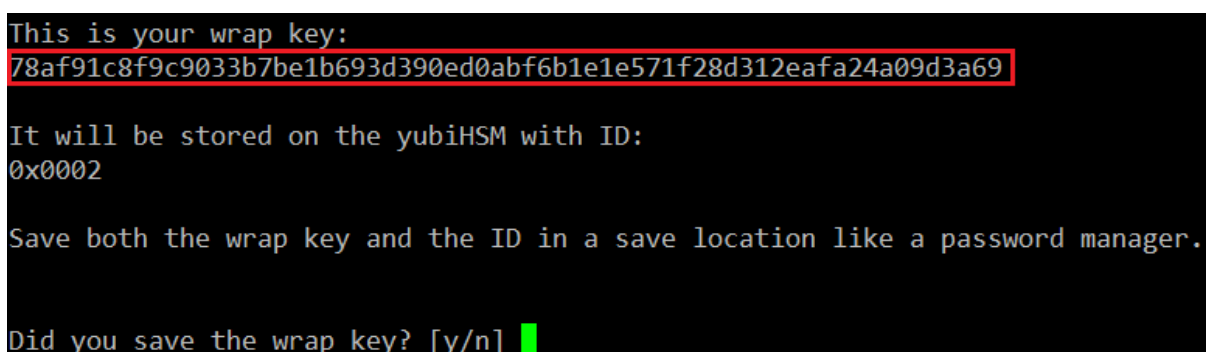
2.7.1 Creating a wrapping key

Now you will be asked to create a wrap key.

A Wrapkey is a secret key used to wrap and unwrap Objects during the export and import process.



Select "Yes"



You now will get a randomly generated wrapping key similar looking to the one shown above.

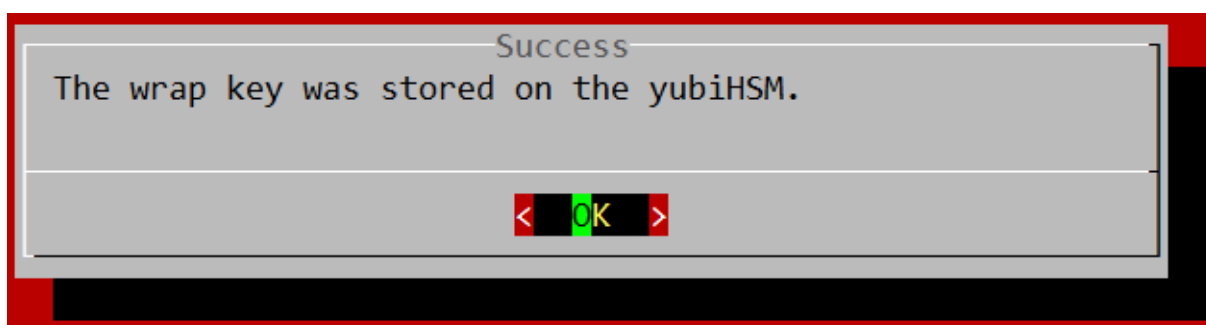
You will need this information to be able to make backups of your YubiHSM!

Note: You can use up to 16 separated PKI servers on one YubiHSM, with this wrapping you can backup all of them at once.

To confirm you have the correct wrap key you will be asked to input it in the next screen.

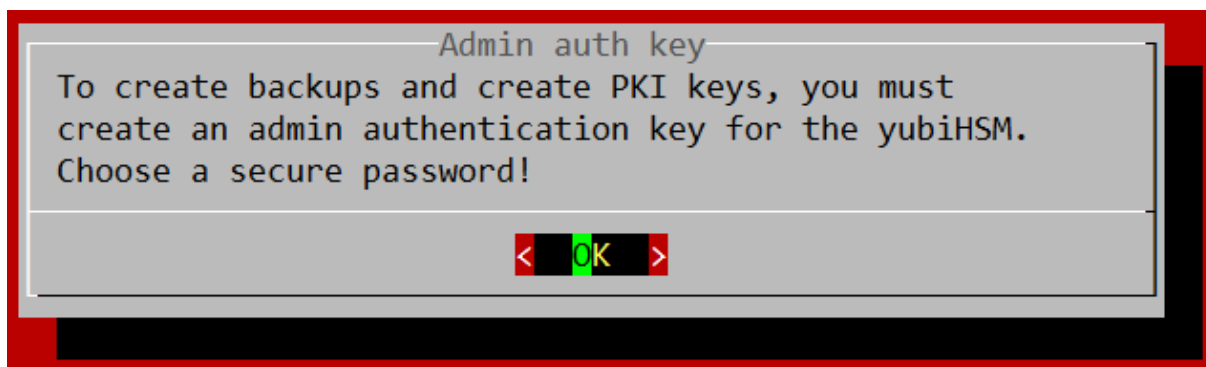
Note: If you use PuTTY, you can highlight text to copy it and right-click to insert it.

After successfully confirming the wrap key it will be stored on the YubiHSM and you will see the following message:



2.7.2 Creating the admin authentication key

Now you will create the admin auth key. This is comparable with a user account and it has an ID (similar to a username) and a password to login.



An Authkey or Authentication Key, is one of the most fundamental Objects there is. Authentication Keys can be used to establish Sessions with a YubiHSM device.

Basically, you can treat authentication keys as users with different rights and abilities.

More info about the different Objects can be found here:

<https://developers.yubico.com/YubiHSM2/Concepts/Object.html>

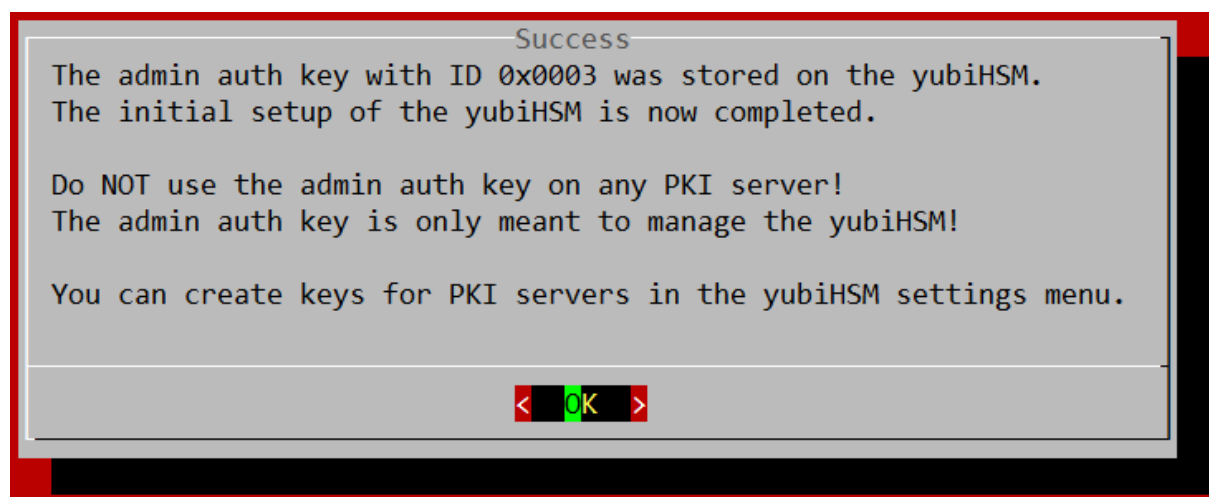
After kicking "OK" you will see this:

```
Please enter the password for the new auth key "Admin auth key" with ID 0x0003 below.
Save both the password and the auth key ID 0x0003 in a save location like a password manager.

Password for the authentication key: █
```

You should choose a very secure (randomly generated) password as this is the admin auth key and is allowed to do almost everything on the YubiHSM.

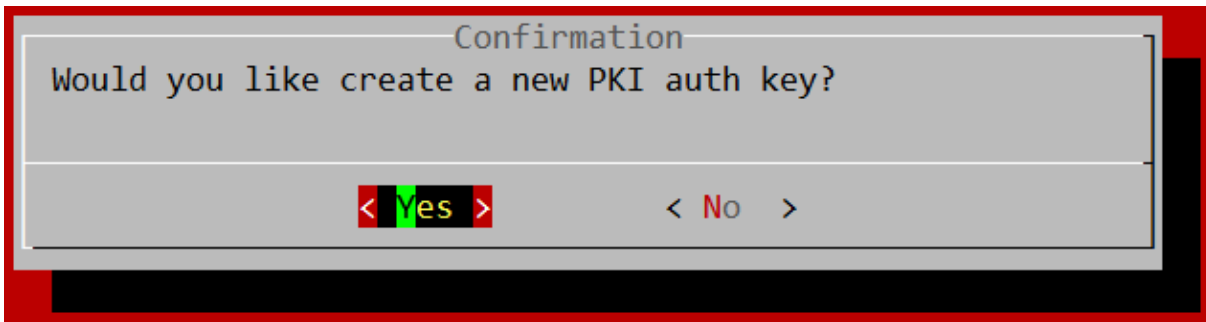
After you confirmed the password you should see this screen:



Now the admin authentication key is saved on the YubiHSM and you can create authentication keys for your PKI servers.

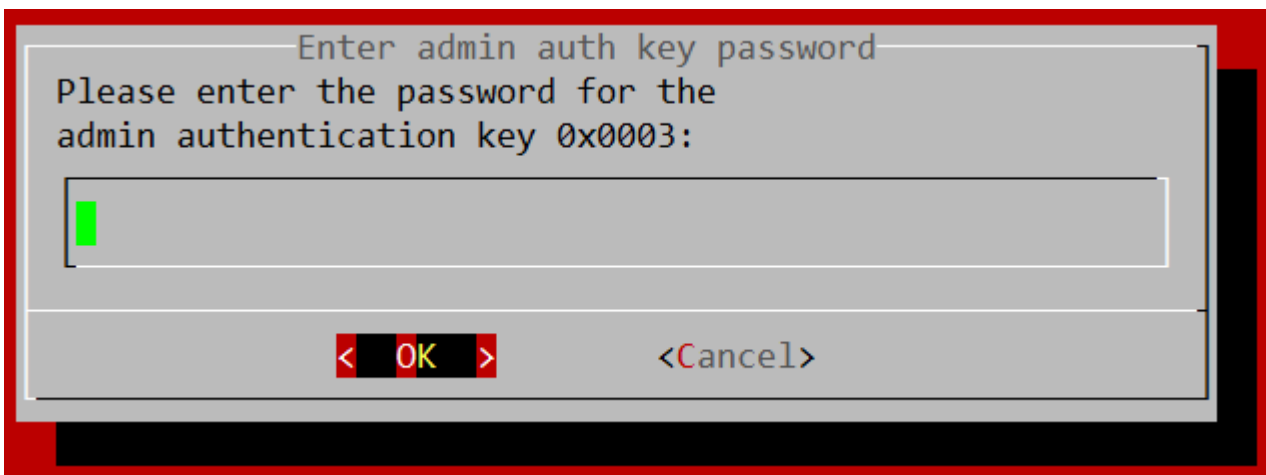
2.8 Creating a PKI authentication key

The wizard will automatically start this for the first key. If you want to create more than one PKI authentication key, you can do so in [The yubiHSM menu](#) after completing the wizard.



Select "Yes".

You can handle the PKI auth keys like user accounts (on the YubiHSM) for your PKI servers.

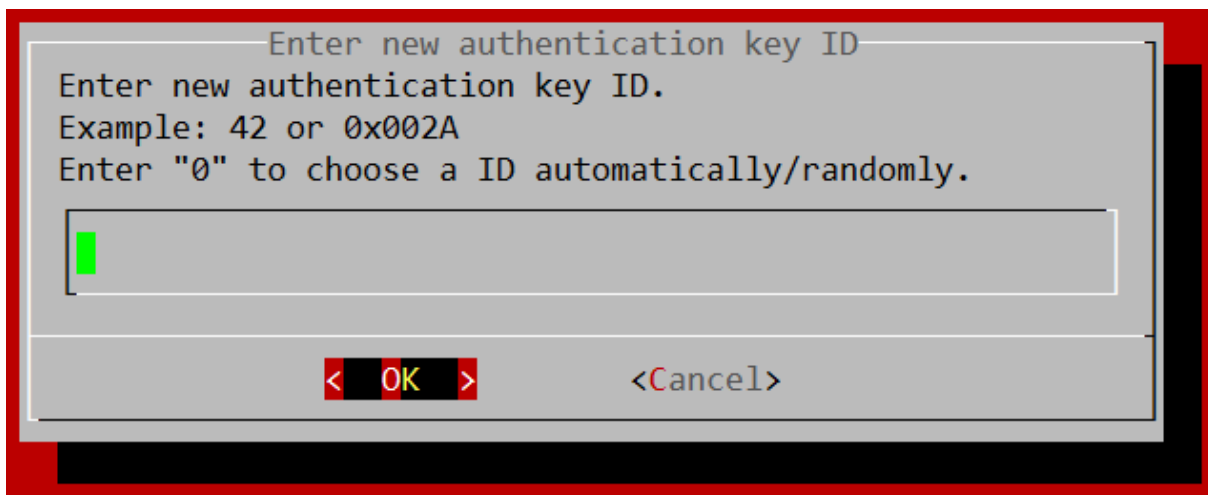


Now enter the password for the admin authentication key you created earlier.

The admin authentication key is the only key that can create new authentication keys for PKI servers.

Note: You can right-click to insert text if you use PuTTY.

2.8.1 Authentication key ID



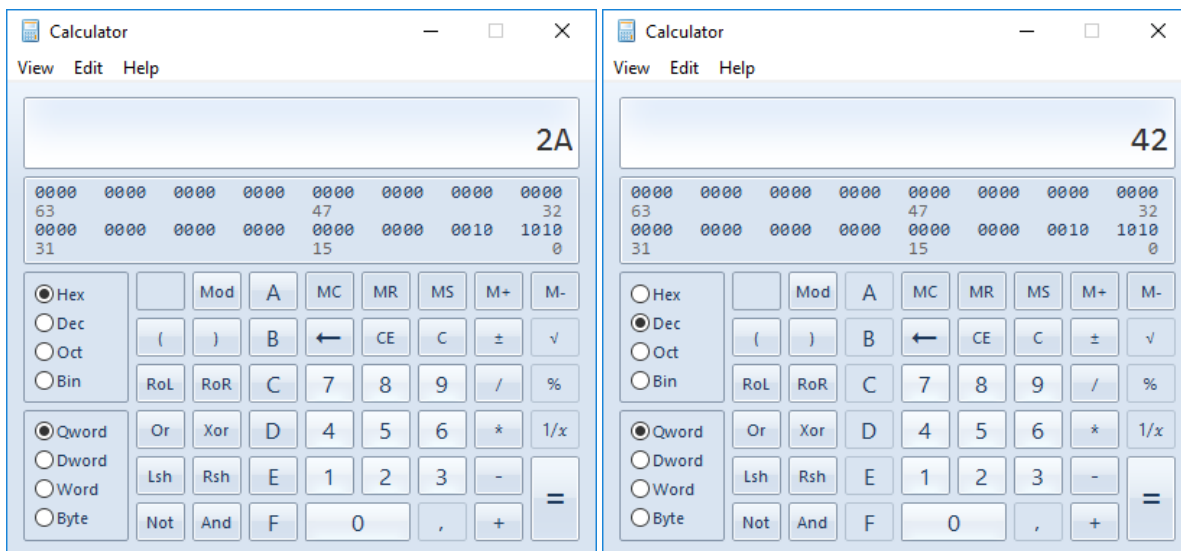
Now you can select an ID for your new PKI auth key. The ID is like a user name.

You can enter a decimal value or a hexadecimal value starting with 0x. Without 0x it is considered as a decimal value.

The range starts at 0x0004 (or just 4 in decimal) to 0xFFFF (65535 in decimal).

With the Windows Calculator in programmer mode (can be changed from the “View” drop-down menu), you can easily convert between decimal and hexadecimal values.

Select “Hex” and input a Hexadecimal number and then select “Dec” to convert it to Decimal. Or the other way around.



Some more info: <https://en.wikipedia.org/wiki/Hexadecimal>

After you entered a ID hit “OK”.

2.8.2 Authentication key label



Enter new authentication key label

Enter new authentication key label.
Example: PKI auth key

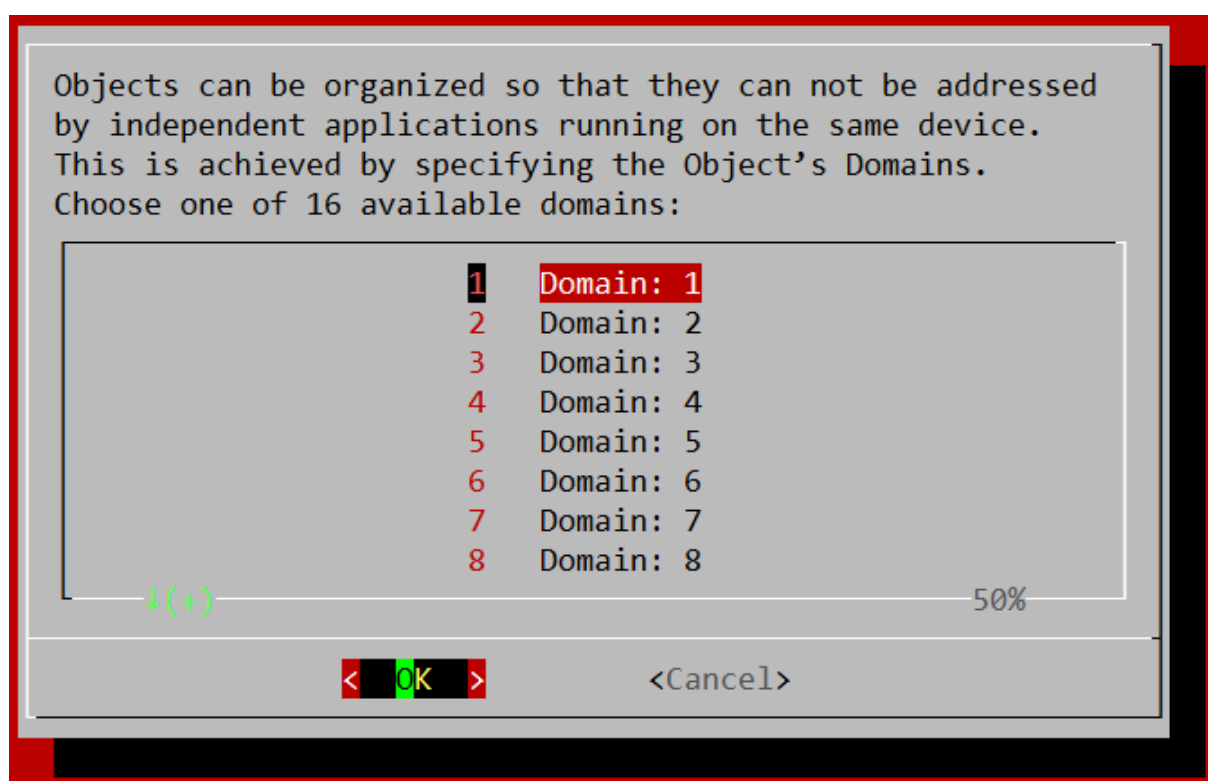
< OK > <Cancel>

Now you can enter a label (name) for the authentication key to easier identify it later.

This can be anything but it is suggested to use the name of the PKI server, followed by “auth key”.
For example: “some-name-01 auth key”.

In the next step you can choose a domain for the authentication key.

2.8.3 Authentication key domain



Objects can be organized so that they can not be addressed by independent applications running on the same device. This is achieved by specifying the Object's Domains. Choose one of 16 available domains:

1	Domain: 1
2	Domain: 2
3	Domain: 3
4	Domain: 4
5	Domain: 5
6	Domain: 6
7	Domain: 7
8	Domain: 8

↓(+)

50%

< OK > <Cancel>

You should select a different domain for each PKI server, otherwise they will have access to the keys from each other.

Choose “1” for the first PKI server, “2” for the second PKI server and so on.

More info about Domains can be found here:

<https://developers.yubico.com/YubiHSM2/Concepts/Domain.html>

2.8.4 Choose a password

Next you can enter the password for the authentication key.

```
Please enter the password for the new auth key "example" with ID 0x002A below.
Save both the password and the auth key ID 0x002A in a save location like a password manager.
Password for the authentication key: █
```

This ID and password will be needed later on the PKI server to access the YubiHSM.

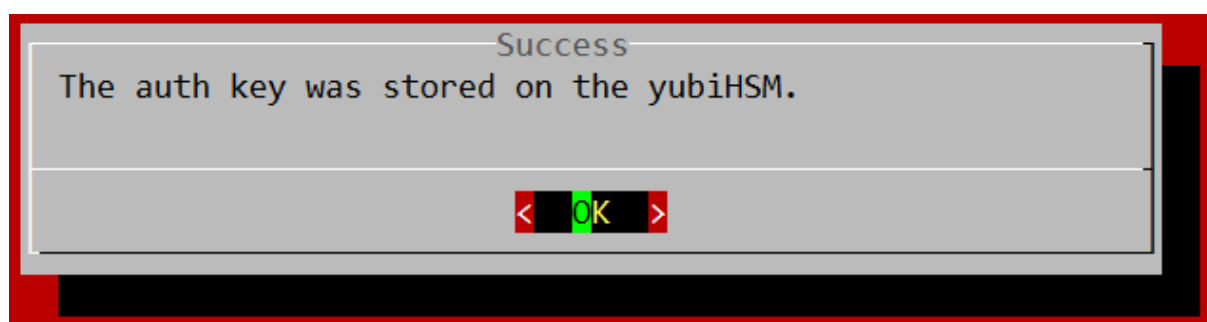
After entering the password, you will see the progress of creating the authentication key on the YubiHSM like shown below.

2.8.5 PKI authentication key stored on the YubiHSM

```
Using default connector URL: http://127.0.0.1:12345
Session keepalive set up to run every 15 seconds
Created session 0
Stored Authentication key 0x002a
OK ID: ^^^^^^
You will need the ID shown above to access this authentication key in the future!
Did you save the ID? [y/n] █
```

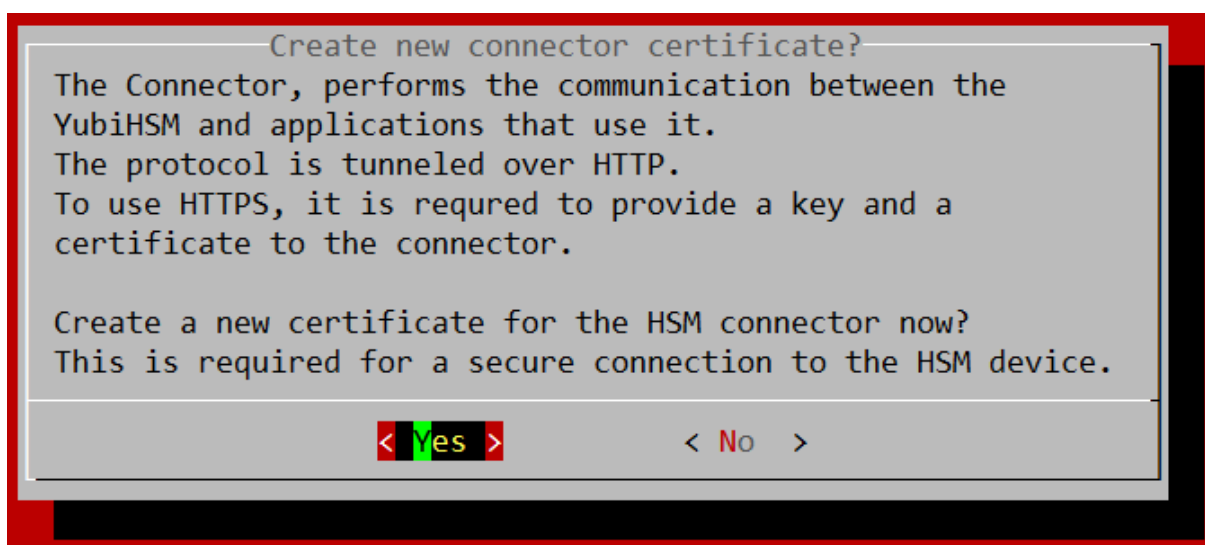
The ID shown here should match the ID you entered earlier. If you have decided to create an ID randomly, it will be displayed here. The ID and the previously entered password belong together. Save both.

Enter "y" to proceed.



2.9 Creating a new connector certificate

Next the certificate for the connector should be created as follows.



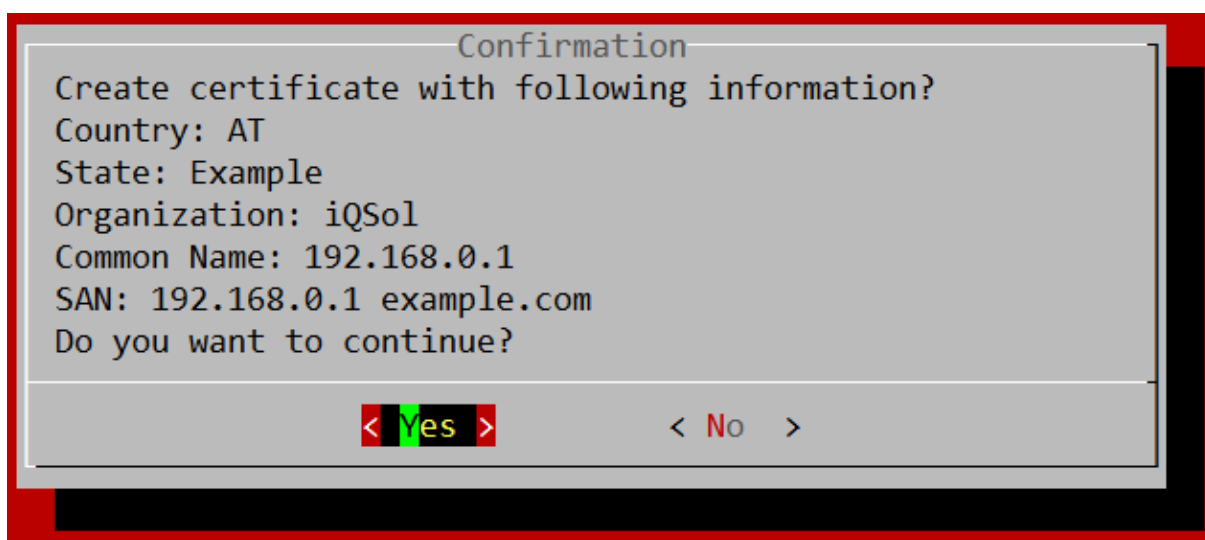
This certificate is not stored on the YubiHSM and is only required for a secure connection from the PKI server to the HSA. (It is used for the nginx HTTPS proxy between the Windows CNG Key Storage Provider and the YubiHSM connector.)

Select "Yes" and proceed with the wizard.

The wizard prompts you for the following information:

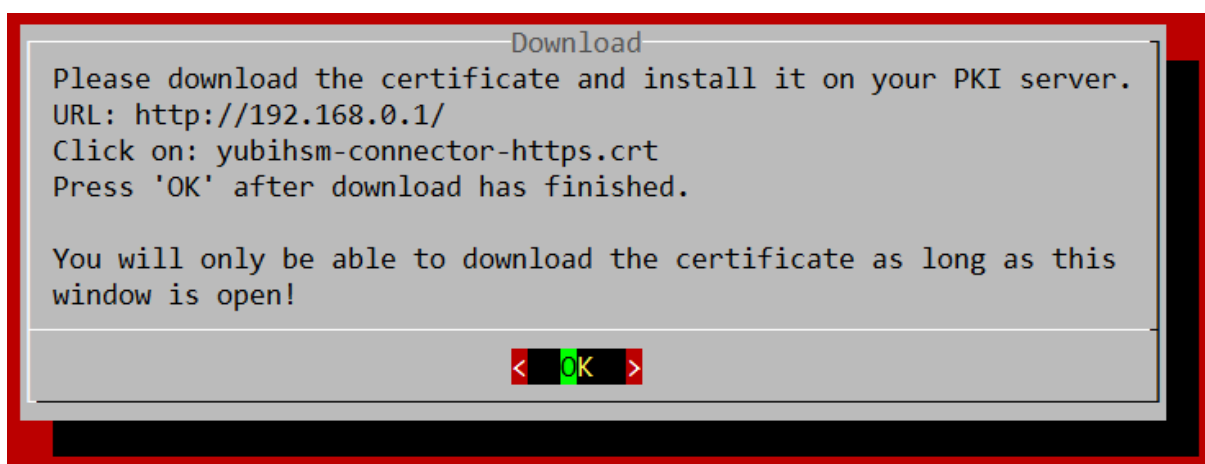
- Country Code
- State
- Organization
- Common Name
- Subject Alt Name

Afterwards you can check the entered information and confirm that everything is correct.

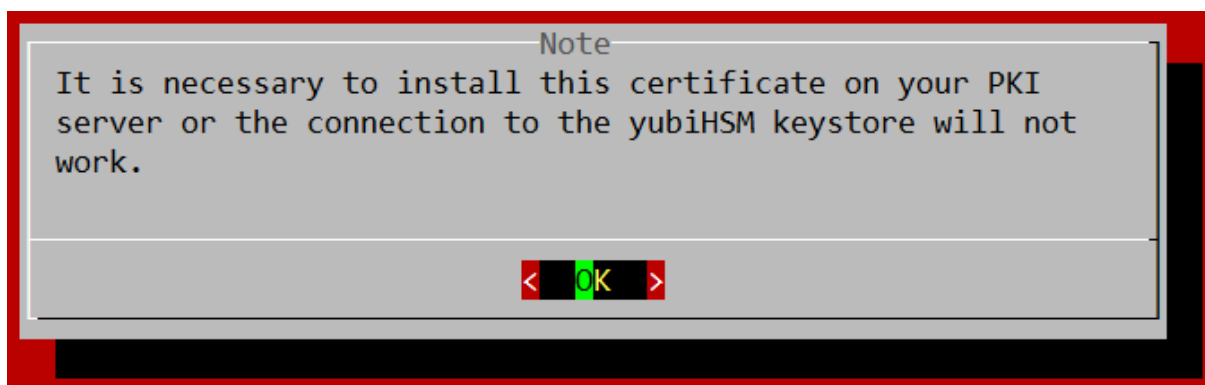


Select "Yes".

Now the certificate will be generated, and you can download it.

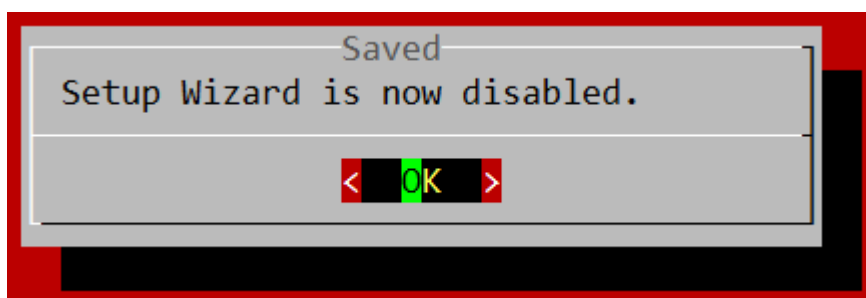


Open a web browser and enter the IP of your HSA (displayed in the “Download” window) in the address bar. Right click on “yubihsm-connector-https.crt” and select “Save target as ...”.



After you have downloaded the certificate, the wizard is complete and disables itself.

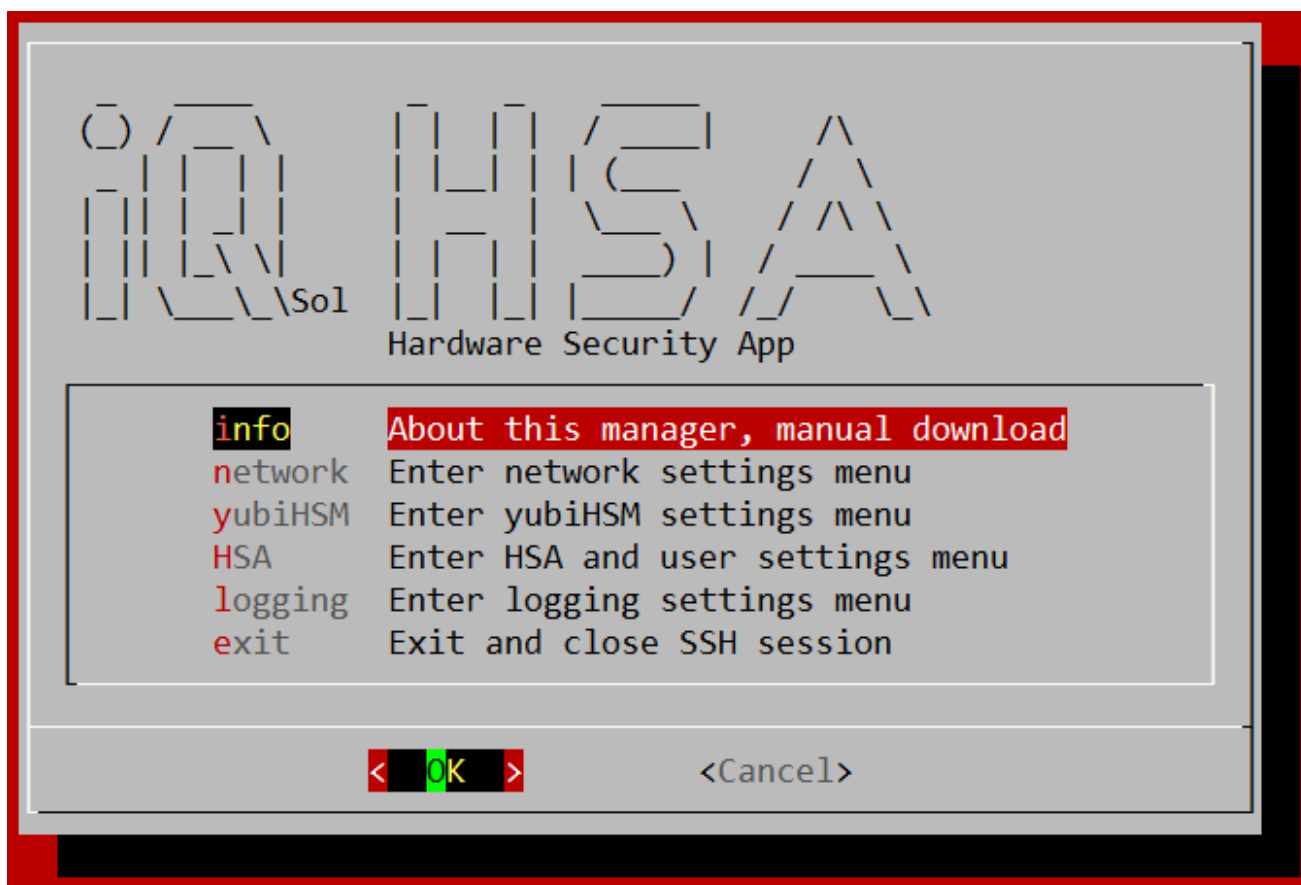
2.10 Wizard completed



It won't start the next time you log in, but the main menu will be displayed instead.

Please read [YubiHSM setup on a PKI Server](#) for detailed information about setting up the YubiHSM CNG Key Storage Provider on Windows.

3 The main menu



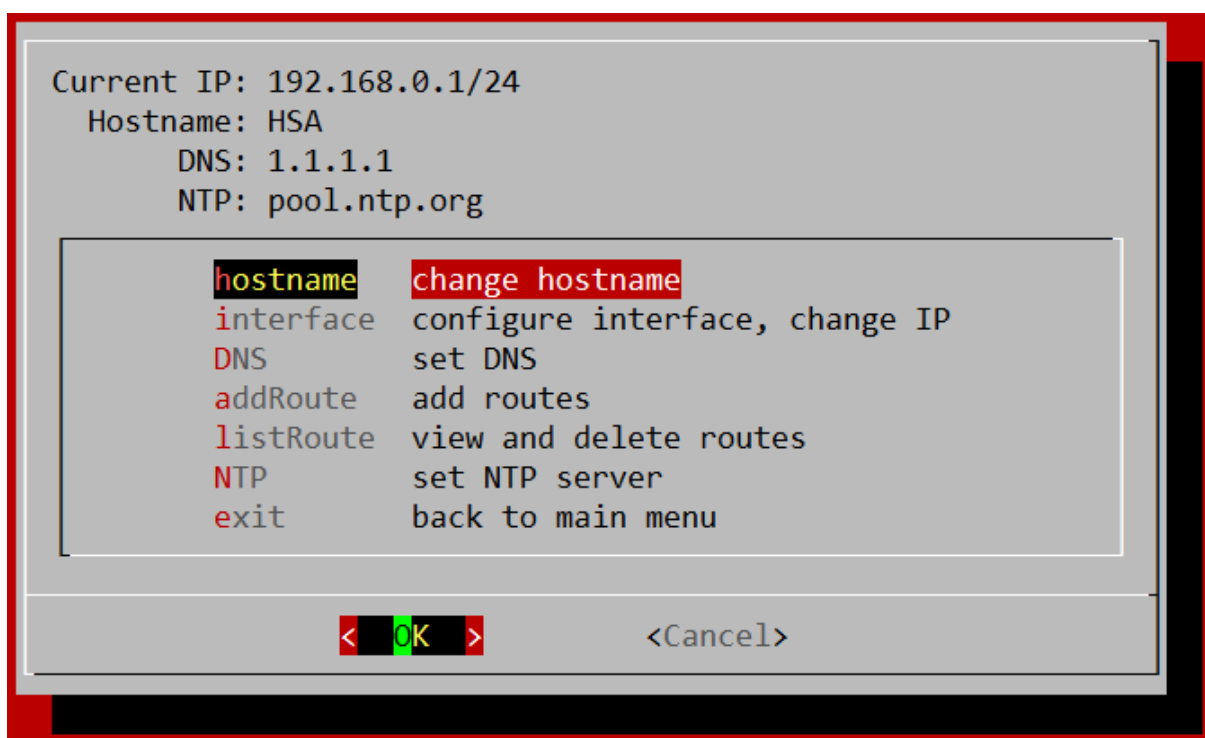
All the settings made by using the [Setup Wizard](#) can also be changed using the menu.

- The entry “info” views some basic information about the device and software and has the option to download the HSA User Manual.
- In the “network” submenu you can find all network related settings: [The network menu](#)
- In the “yubiHSM” submenu you can find settings related to the YubiHSM module: [The yubiHSM menu](#)
- “HSA” contains settings for the HSA Box itself: [The HSA menu](#)
- In “logging” you can change logging related settings: [The logging menu](#)

The menu has a description for each setting and is organized according to the above categories.

There will be safety checks for each setting to avoid mistakes. You can safely navigate through the menus and have a look at the various options.

4 The network menu



This menu provides a brief overview of the most important network settings at the top. In the field below you can change the setting.

4.1 hostname

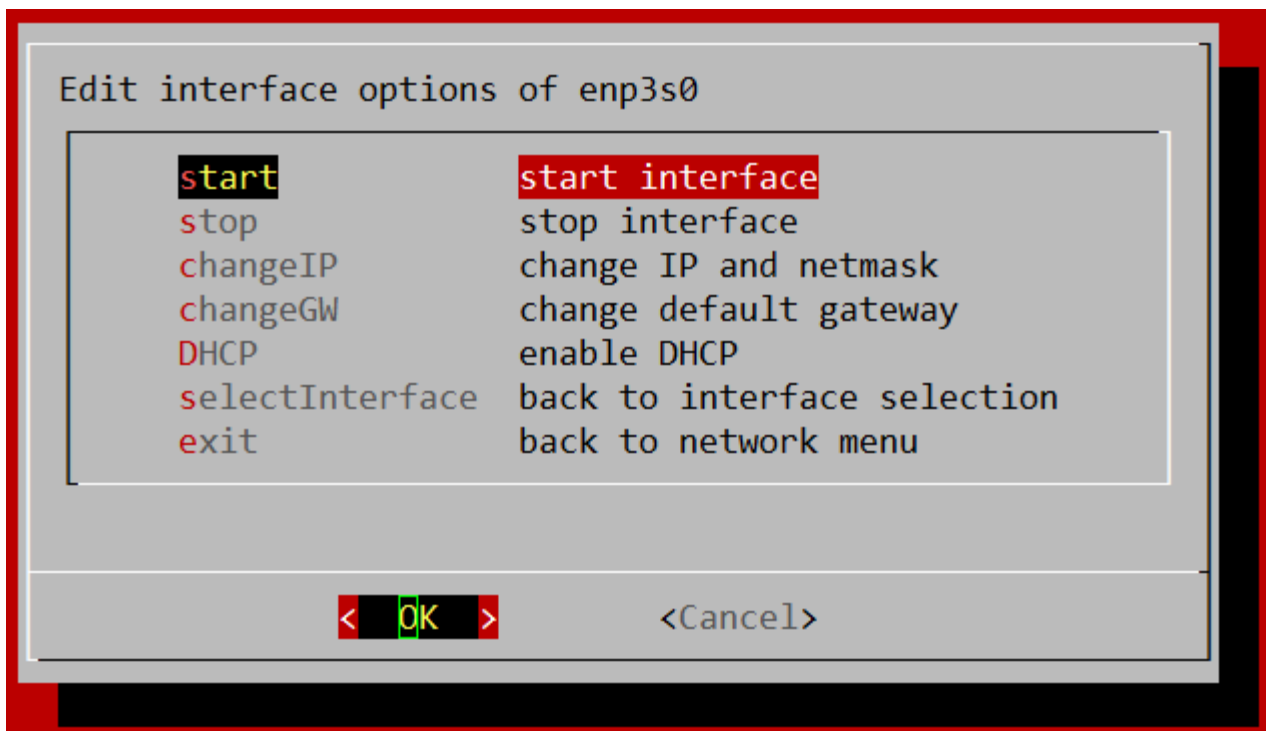
You can change the system host name to make it easier to identify on the network.

4.2 interface

Here you can see available network interfaces (only one on a standard HSA) and some statistics such as the connection speed.

If you select an interface and click OK, you can invoke the Edit interface submenu to make changes to the interface.

4.2.1 Edit interface



- “start” and “stop” should only be used if you are connected via HDMI and a USB keyboard or you will lose the connection to the HSA.
- “changeIP” also requires the input of a gateway so as not to lose the connection with the device.
- With “changeGW” you can change the gateway independently.
- DHCP: It is not recommended to enable the DHCP client, but if your network requires it, you can do so, but make sure that your DHCP server gives a fixed IP to the HSA.

4.3 DNS

You can use an internal DNS server to find local servers on the network via hostnames.

4.4 addRoute

Add routes to the routing table.

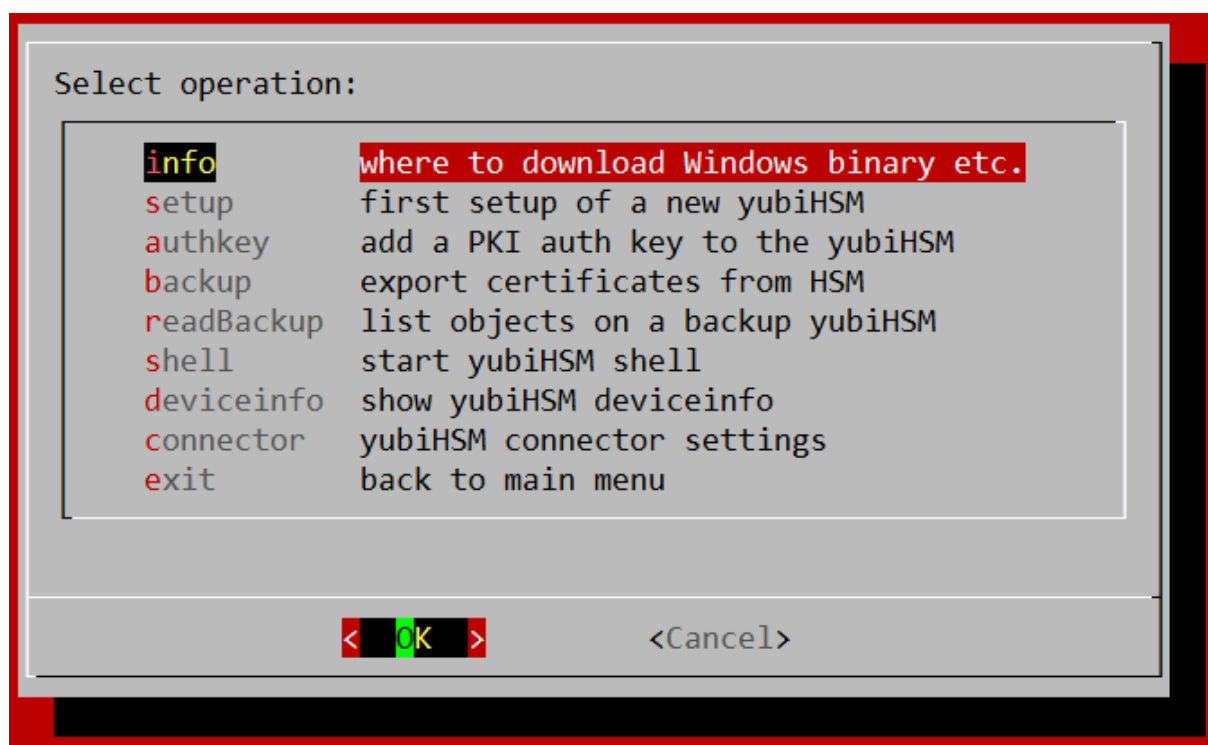
4.5 listRoute

List all currently enabled routes, select one and click OK to delete it or select Exit to go back.

4.6 NTP

You can use an NTP server on the local network.

5 The yubiHSM menu



5.1 info

Contains some basic info and useful links about the YubiHSM.

5.2 setup

This is the same as in the [Setup Wizard: Setup of a new YubiHSM](#)

5.3 authkey

This is the same as in the [Setup Wizard: Creating a PKI authentication key](#)

5.4 backup

Allows you to copy all objects stored on the main YubiHSM to a backup device.

To make a backup, follow the onscreen instructions.

Note: A backup using this assistant is only possible if the [Setup of a new YubiHSM](#) has been completed.

This does not include the config from the HSA, see [The HSA menu](#) > [backup](#) to create config backups.

5.5 readBackup

You can display the objects stored on an external YubiHSM. To do this, you must enter the ID of the admin authentication key (0x0003 on a YubiHSM configured with the HSA), the password for this key, and the serial number of the YubiHSM.

5.6 shell

Starts the YubiHSM Shell. More details about the shell can be found here:

https://developers.yubico.com/YubiHSM2/Component_Reference/yubihsm-shell/

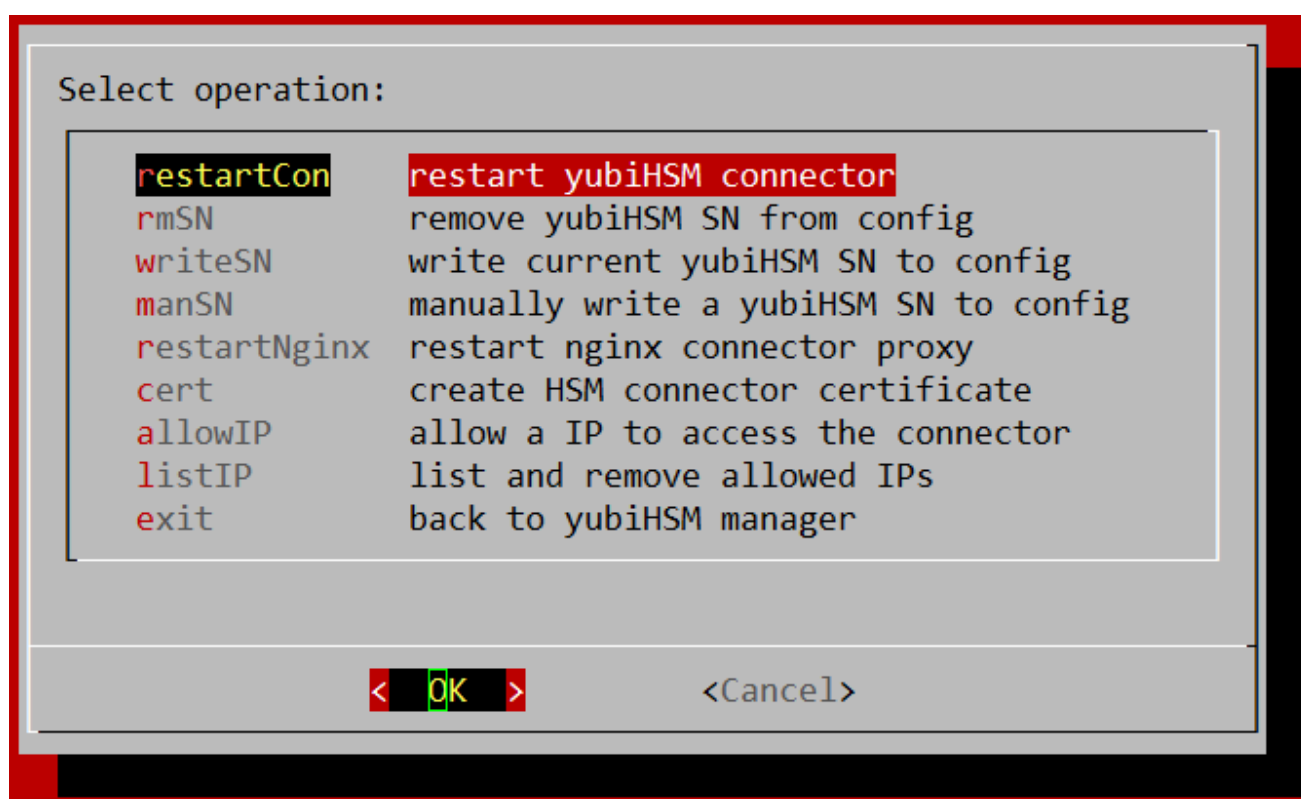
Note: You should always use the menus provided by the HSA to configure a YubiHSM to avoid compatibility issues.

5.7 deviceinfo

Shows some basic information about the YubiHSM in the HSA, such as the serial number.

5.8 connector

Opens a submenu:



5.8.1 restartCon

Restarts the YubiHSM connector on the HSA.

More info about the YubiHSM connector:

https://developers.yubico.com/YubiHSM2/Component_Reference/yubihsm-connector/

5.8.2 rmSN

Deletes the YubiHSM serial number from the connector config.

5.8.3 writeSN

Writes the serial number of the currently connected YubiHSM to the connector configuration file.

This is required if multiple YubiHSM modules are connected to the HSA to identify the main device.

Note: The Setup Wizard configures this automatically. This is only required if you replace your YubiHSM or did not complete the Setup Wizard.

5.8.4 manSN

This is like writeSN, but you can enter a serial number manually.

5.8.5 restartNginx

Restarts the nginx HTTPS proxy for the YubiHSM connector.

For details about the nginx proxy see: Creating a new connector certificate

5.8.6 cert

This is the same as in the Setup Wizard: Creating a new connector certificate

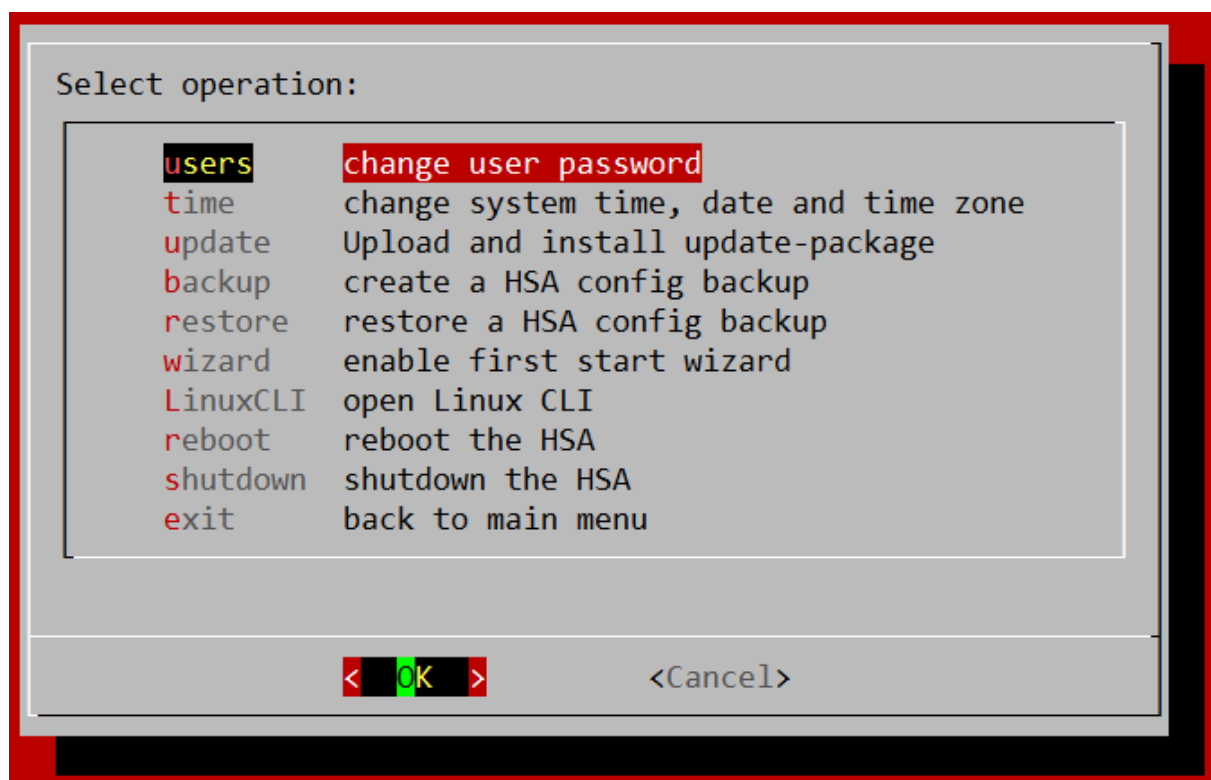
5.8.7 allowIP

You can specify which IPs are allowed to connect to the YubiHSM connector.

5.8.8 listIP

Displays all allowed IPs specified with allowIP, select one and click OK to remove it or select Exit to go back.

6 The HSA menu

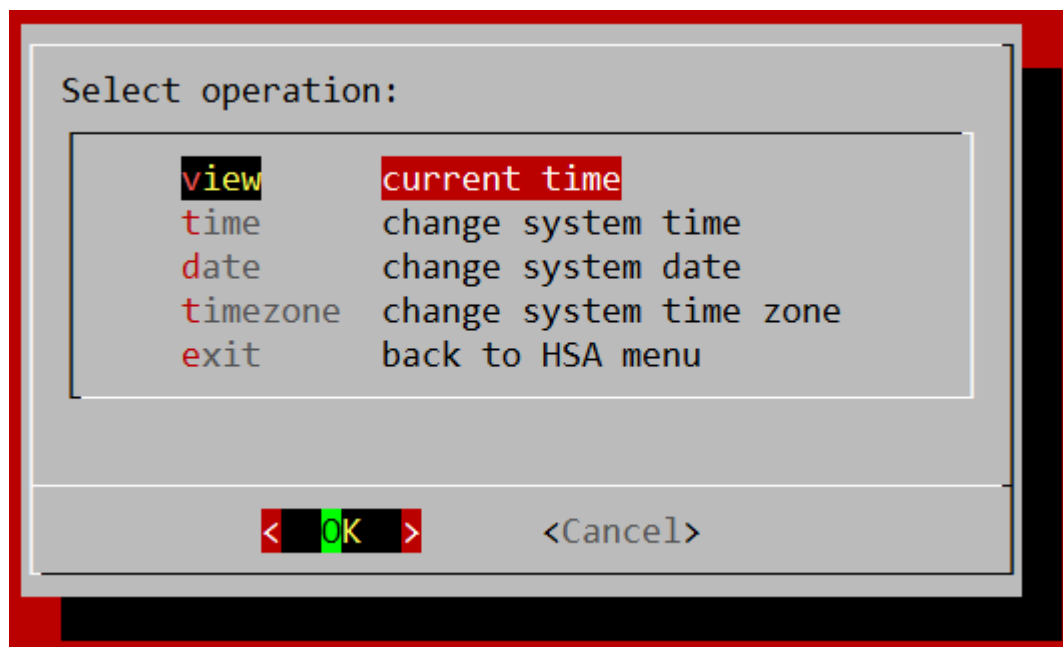


6.1 users

Opens a small submenu where you can select a user (deviceadmin or root) to change the password.

6.2 time

Opens a submenu:



These settings are the same as made with the Setup Wizard: Enter time, Enter date, Setting timezone.

6.3 update

Please follow the onscreen instructions to install offline updates for the HSA.

Updates can be downloaded via the FTP:

<ftp://customer:FZig9k@ftp2.iqsol.biz/6-IQSol-Customer/HSA/Updates/>

6.4 backup

This option allows you to create and download a configuration backup from the HSA.

After a backup file has been created, you can download it. Open a web browser and enter the IP of your HSA (displayed in the “Download” window) in the address bar. Right click on “backup_date_time.tar.gz” and select “Save target as ...”.

The backups will be named according to the following scheme: backup_DATE_TIME.tar.gz

Example: backup_20180828_143021.tar.gz (2018.08.28 14:30:21)

Note: This does NOT include user passwords on the HSA and certificates and keys stored on the yubiHSM! See The yubiHSM menu > backup to create a backup from the YubiHSM.

6.5 restore

Please follow the onscreen instructions to restore backups to the HSA.

6.6 wizard

This enables or disables the Setup Wizard.

6.7 LinuxCLI

This opens a Linux Shell.

Note: You should always use the menus provided by the HSA to make configuration changes to avoid compatibility issues.

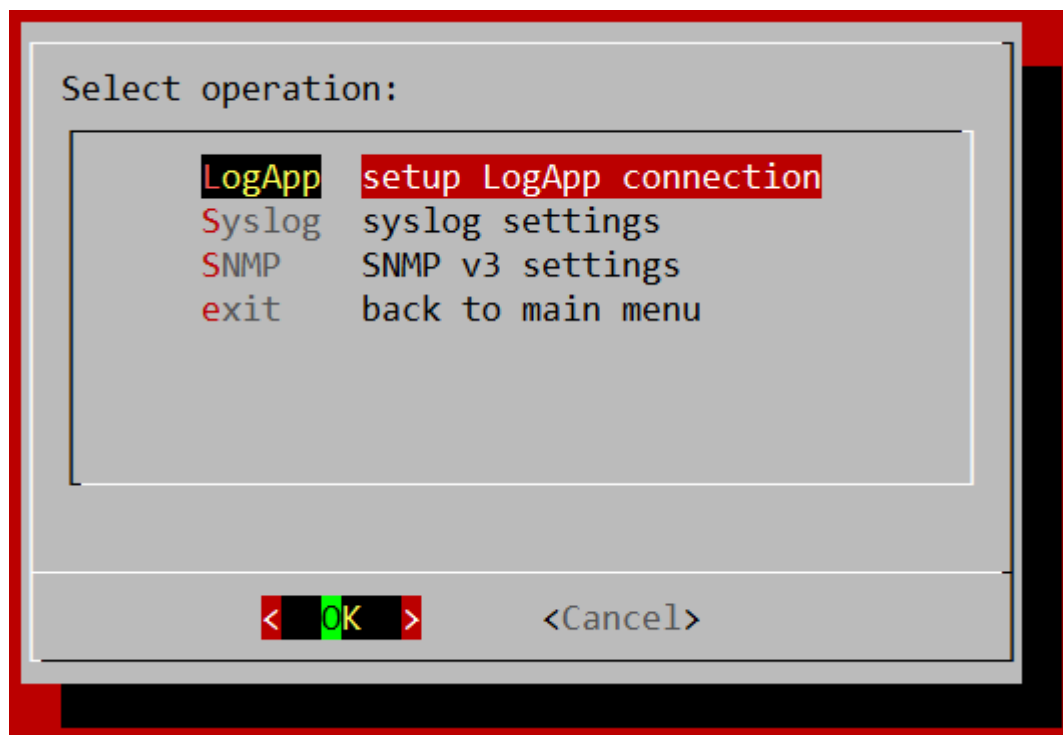
6.8 reboot

Reboots the HSA.

6.9 shutdown

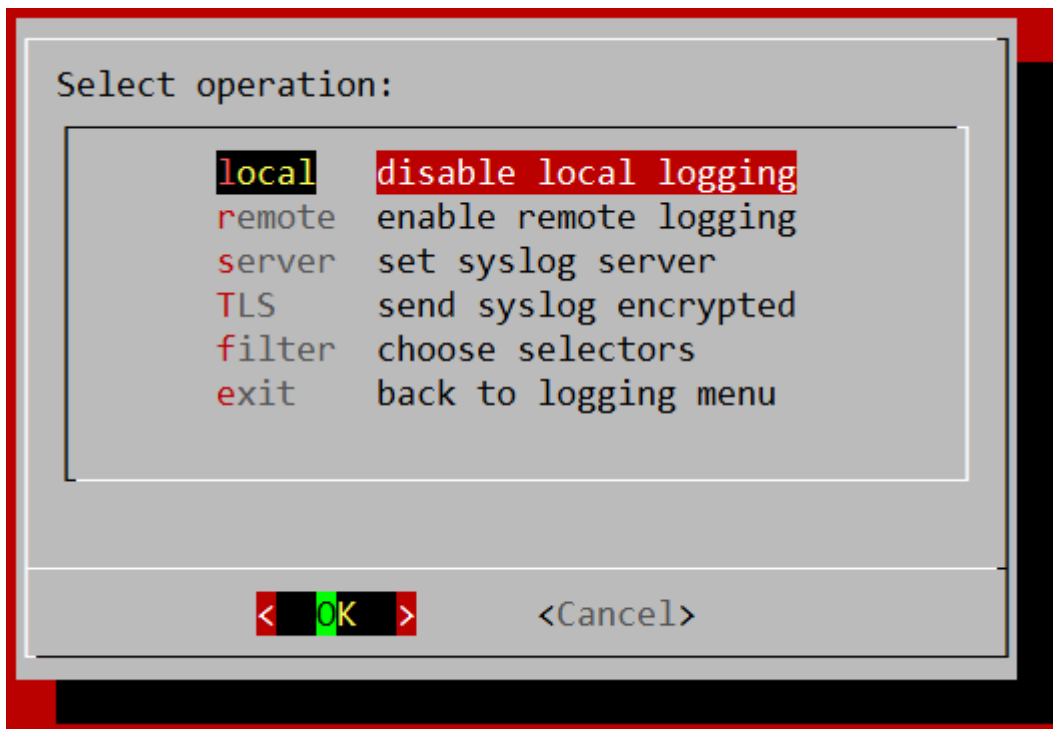
Shutdown the HSA.

7 The logging menu



7.1 Syslog

Opens a submenu:



7.1.1 local

Toggles between enabled or disabled local logging.

7.1.2 remote

Toggles between enabled or disabled logging to a remote syslog server.

7.1.3 server

Here you can specify how to connect to the remote syslog server (IP, Port, TCP or UDP).

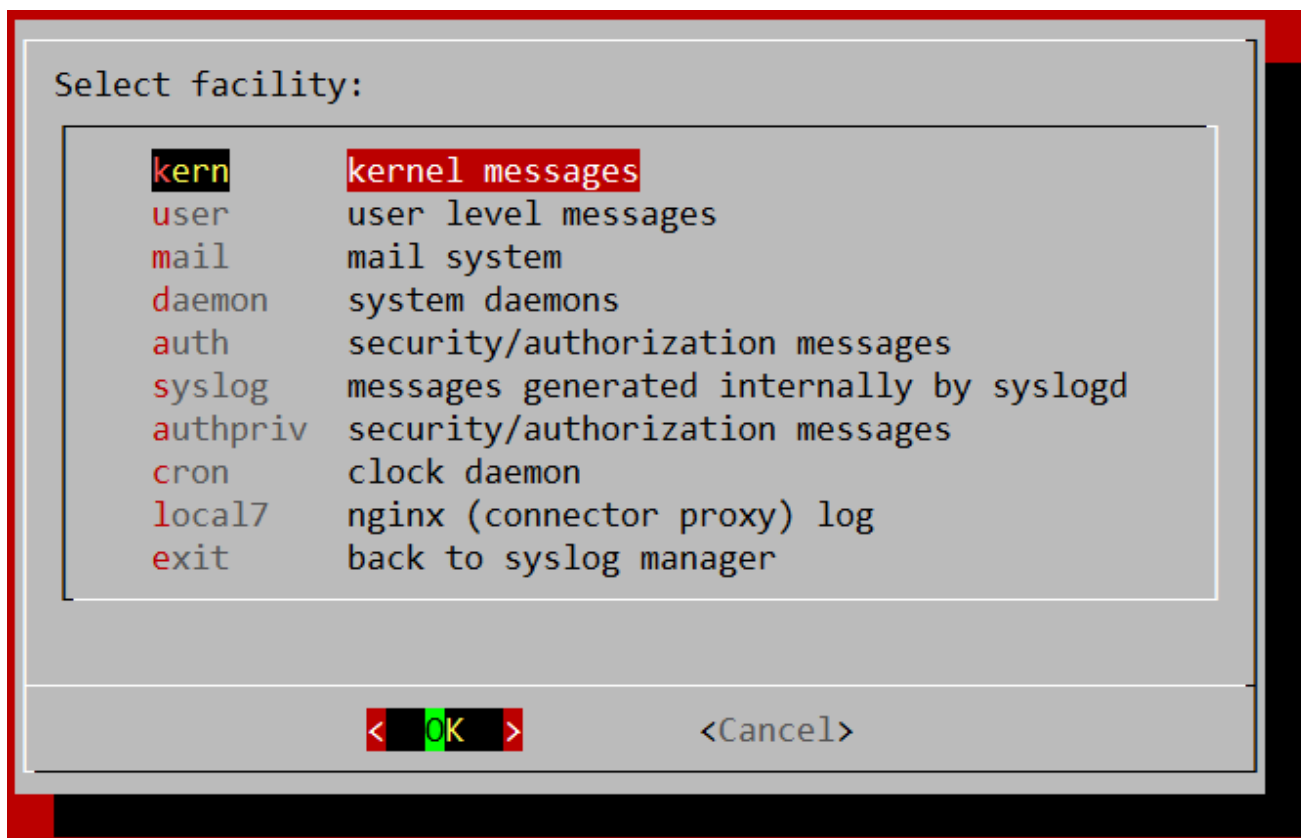
7.1.4 TLS

Opens a submenu where you can configure syslog TLS settings.

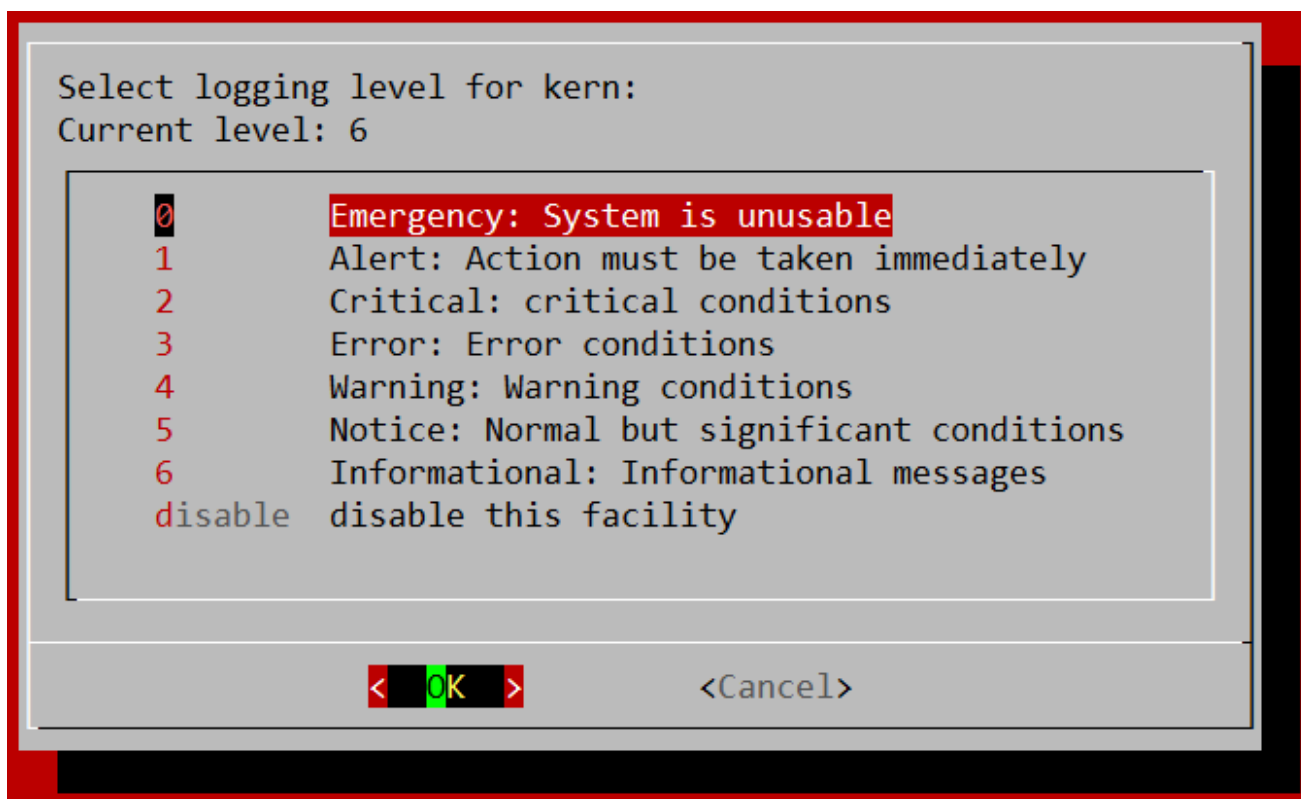
- “upload” the certificate from your syslog server.
- “enable”/“disable” TLS (toggles between enabled or disabled).
- With “AuthMode” you can choose between the following authentication methods:
 - anon - anonymous authentication
 - x509/fingerprint - certificate fingerprint authentication
 - x509/certvalid - certificate validation only
 - x509/name - certificate and subject name validation

7.1.5 filter

Opens a submenu where you can select a syslog facility, to customize its logging level.



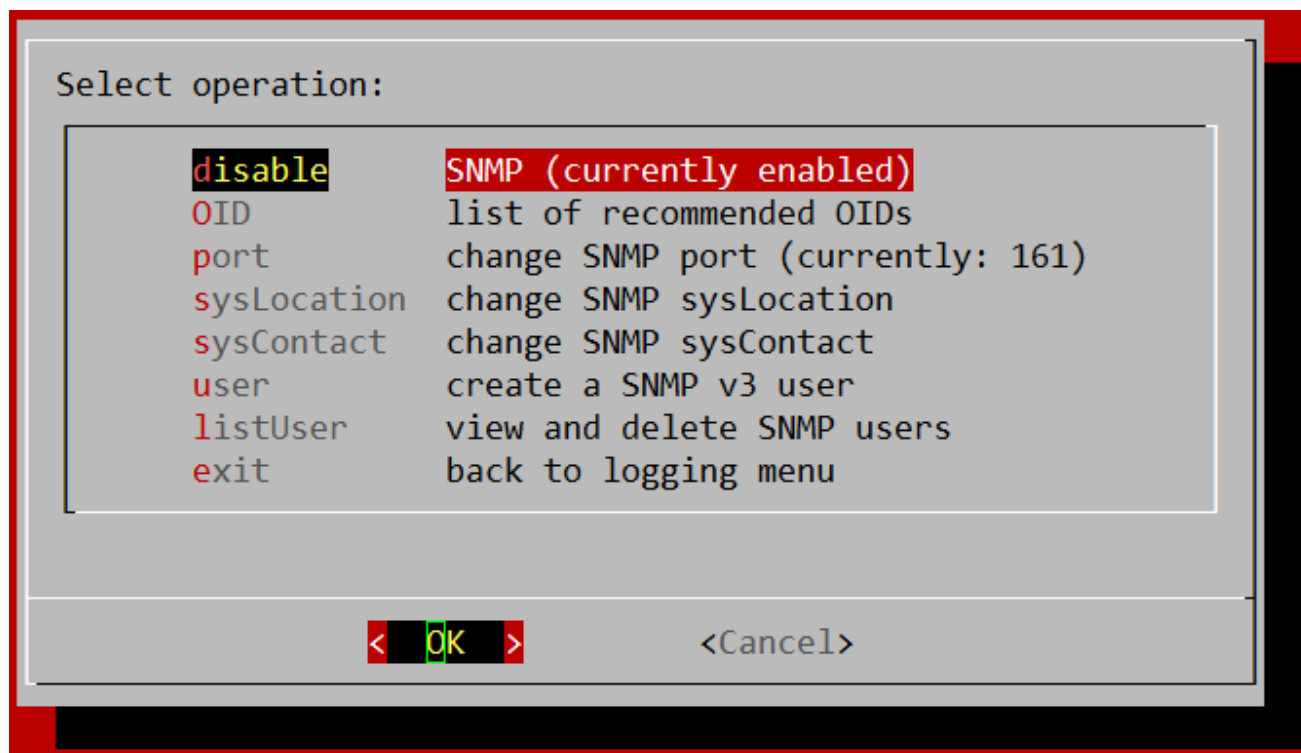
After selecting a facility and clicking OK, the following submenu opens:



Select one of the displayed logging levels and click OK.

7.2 SNMP

Opens a submenu to configure SNMP v3.



7.2.1 enable/disable

Toggle switch.

7.2.2 OID

Displays a list of usefull OIDs (Object Identifiers) for reading information using SNMP.

Example snmpwalk command to check if YubiHSM connector and nginx proxy are running:

```
snmpwalk -v 3 -u user -a SHA -A auth-pw -x AES -X crypto-pw -l authNoPriv 192.168.0.1 .1.3.6.1.4.1.2021.2
```

7.2.3 port

Changes the SNMP port.

7.2.4 sysLocation

Can change the name of the physical location for the device.

7.2.5 sysContact

Can change the the primary contact for the device.

7.2.6 user

Can crate a new SNMP v3 user. The following information is required for this: user name, authentication password (to authenticate the user), crypto password (to encrypt the data).

7.2.7 listUser

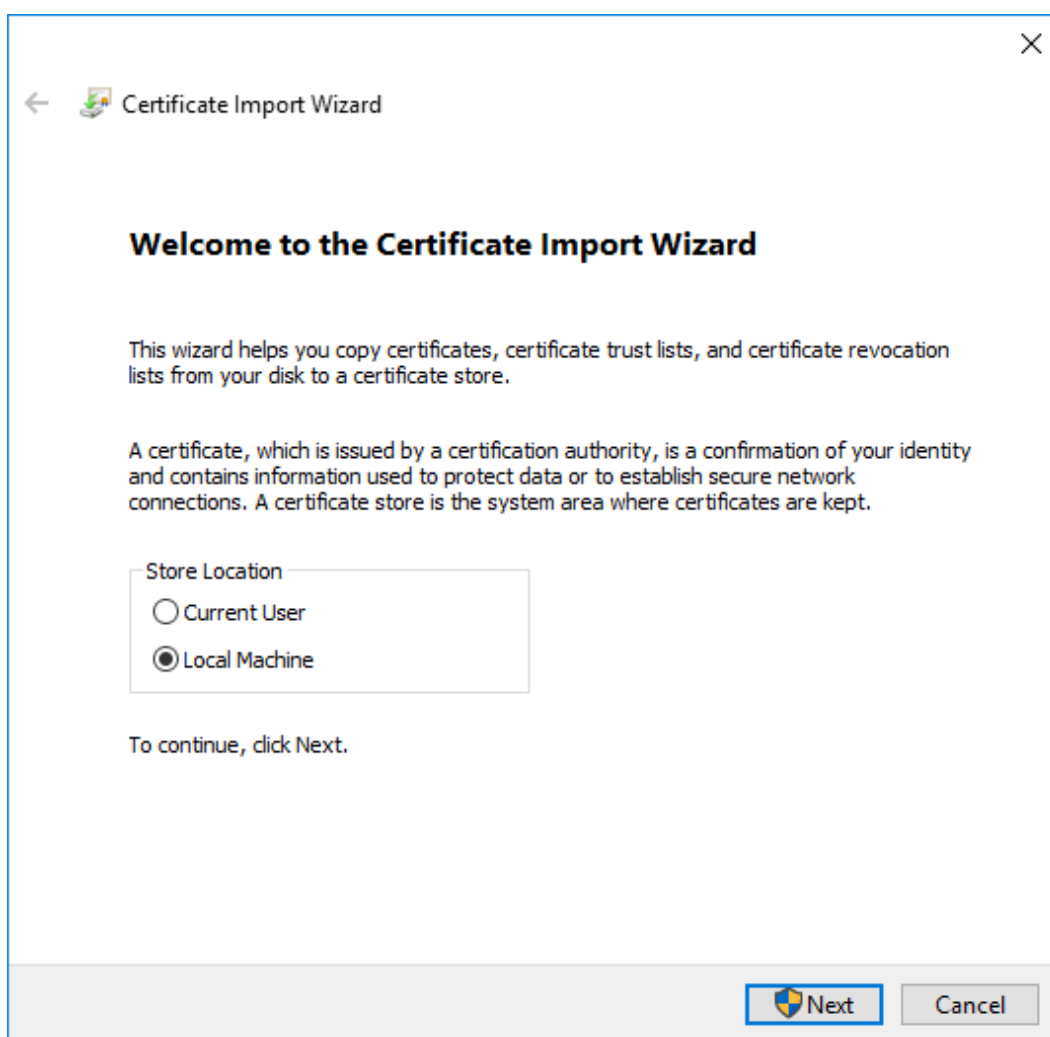
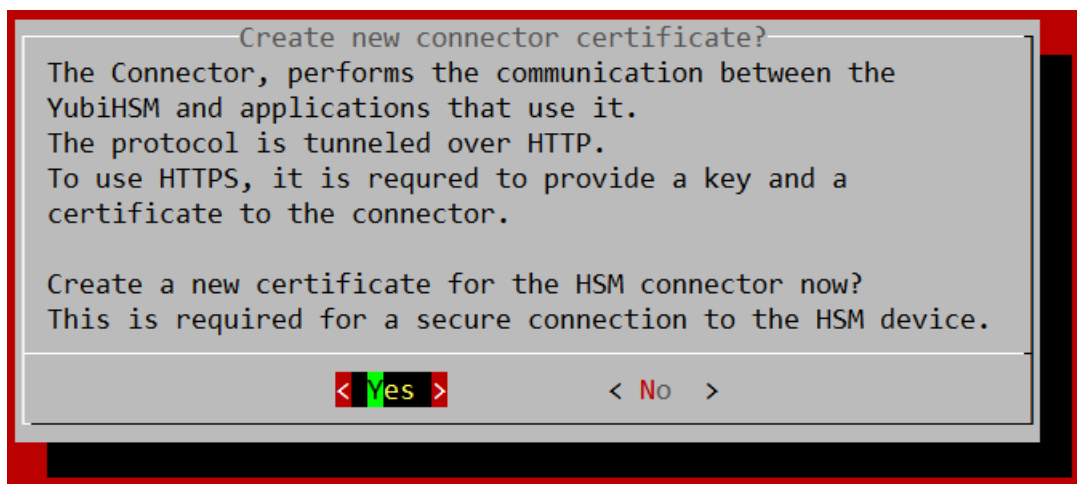
Lists all SNMP v3 users, select one and click OK to delete it or select Exit to go back.

8 YubiHSM setup on a PKI Server

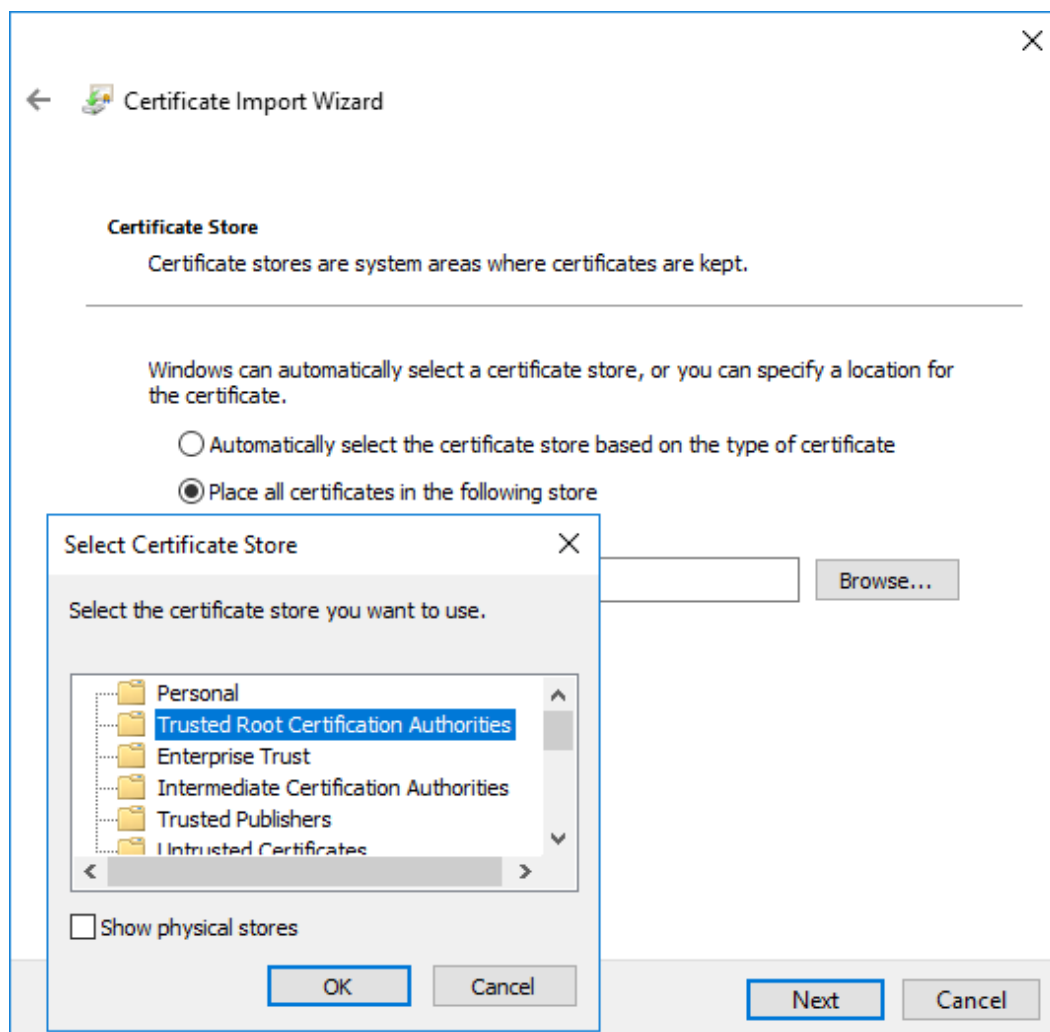
8.1 Installing the connector certificate

First install the connector certificate “yubihsm-connector-https.crt” on the PKI server.

This certificate was created and downloaded on the HSA Box.



Select “Local Machine” and install it in “Trusted Root Certification Authorities”.



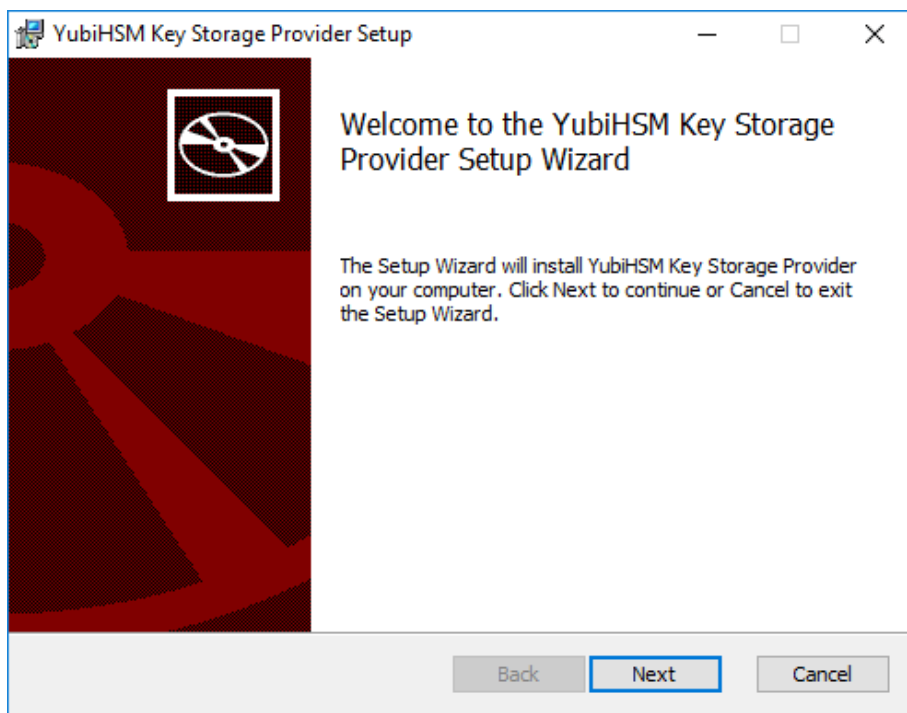
8.2 Installing the YubiHSM Key Storage Provider.

Download the Setup from the following Link:

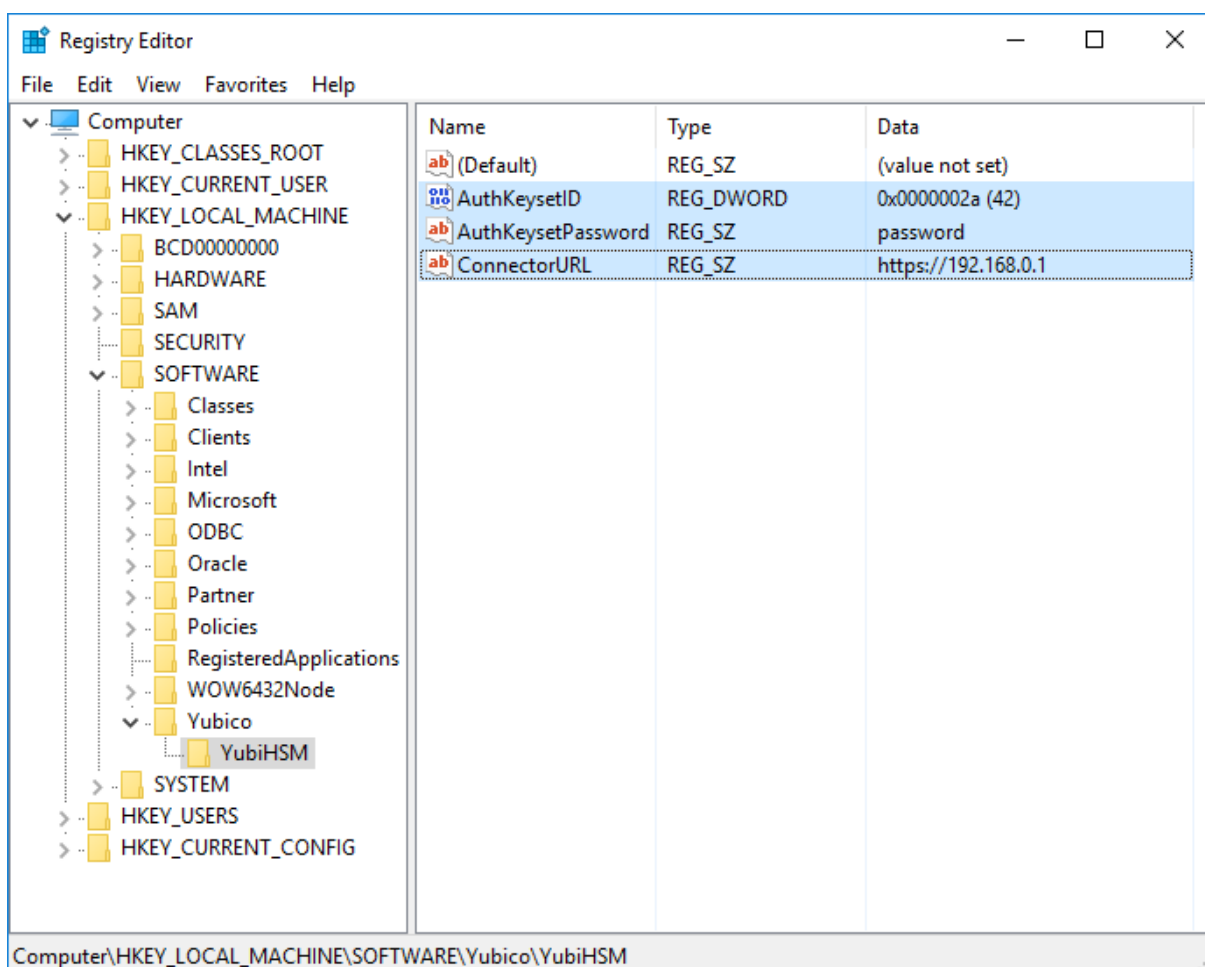
<https://www.yubico.com/products/services-software/download/yubihsm-2-libraries-and-tools/>

Select “Windows 10, Server 2012, Server 2016”.

Extract the zip archive and execute “yubihsm-cngprovider-windows-amd64.msi”, the other contents of the zip are not required.

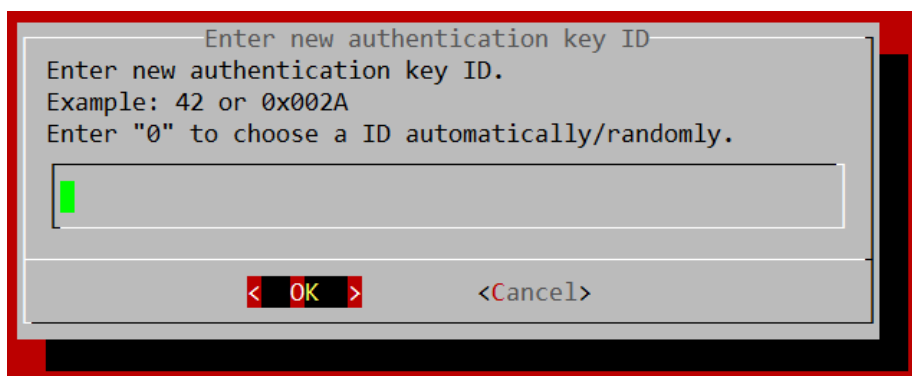


Follow the YubiHSM Key Storage Provider Setup Wizard until it is completed and then open the Registry Editor and navigate to \HKEY_LOCAL_MACHINE\SOFTWARE\Yubico\YubiHSM.



Change the “AuthKeysetID”, “AuthKeysetPassword” and “ConnectorURL” according to the settings made on the HSA box.

“AuthKeysetID” is the ID for the PKI authentication key created on the HSA box.



This is the information you entered on the HSA box in the following screen:

If you entered “0” then it was shown here:

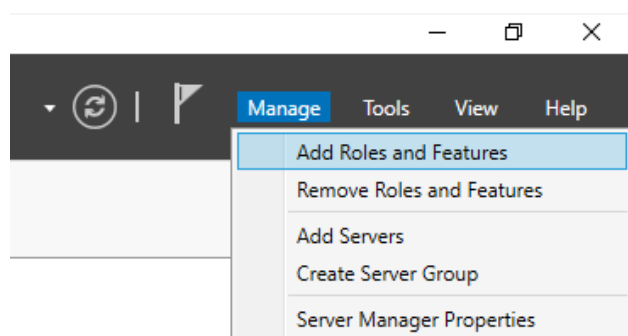
```
Stored Authentication key 0x0058
OK ID: ^^^^^^
You will need the ID shown above to access this authentication key in the future!
```

“AuthKeysetPassword” is the password specified for the authentication key.

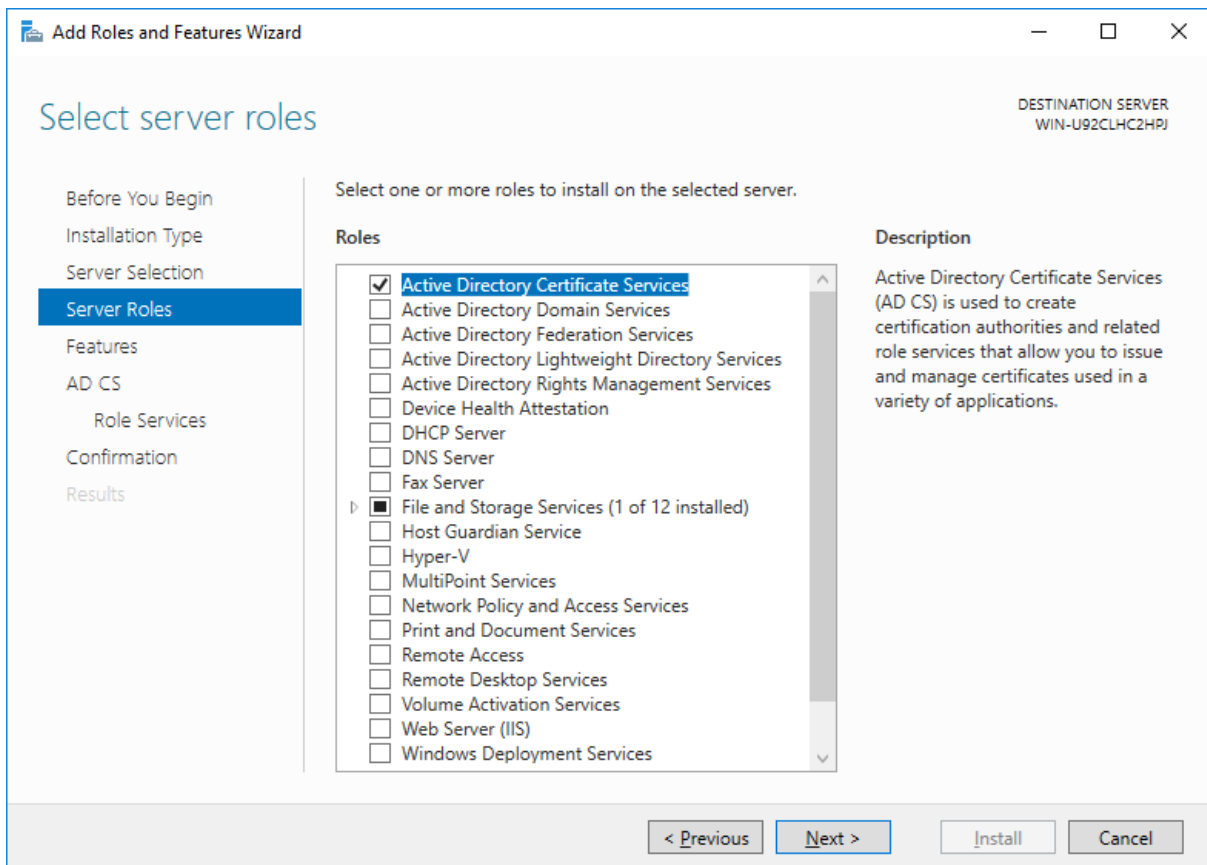
“ConnectorURL” is https:// followed by the IP of the HSA Box

8.3 Add the CA Role

Select Add Roles and Features on the PKI Server.

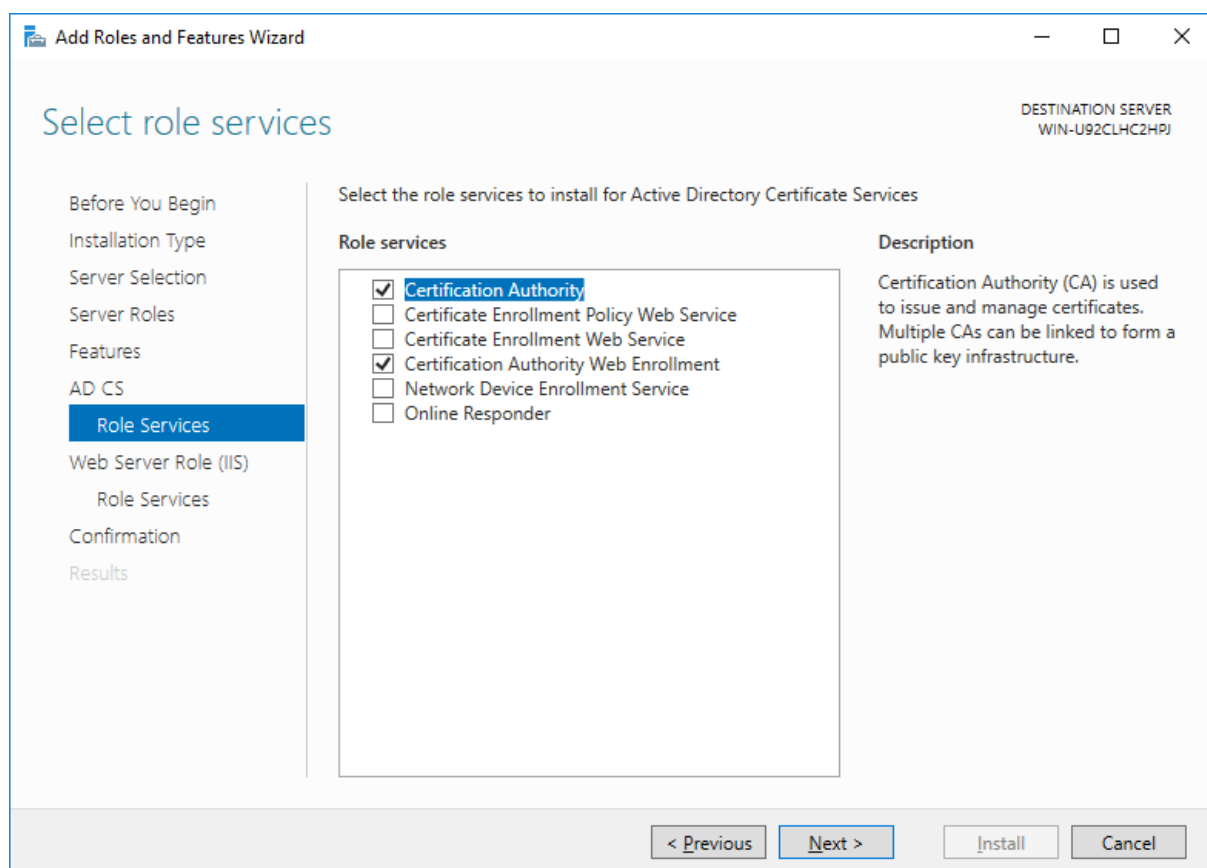


Follow the wizard until “Server Roles” and select “Active Directory Certificate Services”.



Proceed with the wizard.

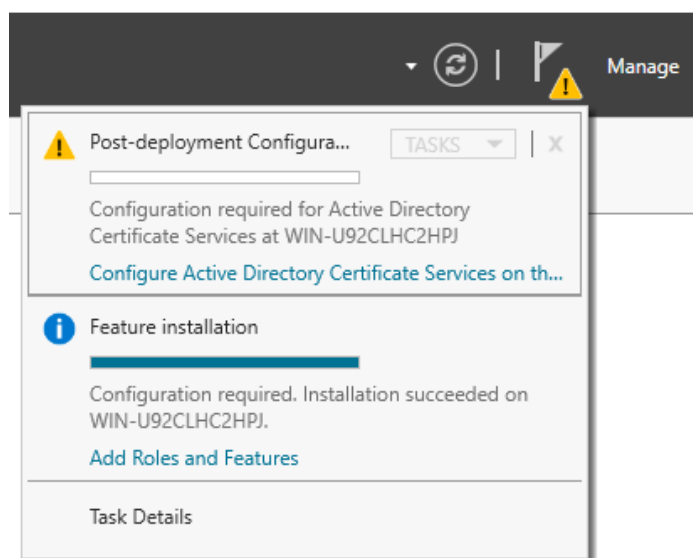
When you reach “Role Services” select “Certification Authority” and “Certification Authority Web Enrollment”.



Proceed with the wizard until it's finished.

8.4 Configure Active Directory Certificate Services

In the "Server Manager" you will see the following in the upper right:



Click on [Configure Active Directory Certificate Services...](#)

A Wizard will start, follow the Wizard and select options as shown below.

AD CS Configuration

Role Services

Credentials

Role Services

Setup Type

CA Type

Private Key

Cryptography

CA Name

Validity Period

Certificate Database

Confirmation

Progress

Results

Select Role Services to configure

☒ Certification Authority
☐ Certification Authority Web Enrollment
☐ Online Responder
☐ Network Device Enrollment Service
☐ Certificate Enrollment Web Service
☐ Certificate Enrollment Policy Web Service

[More about AD CS Server Roles](#)

DESTINATION SERVER

WIN-U92CLHC2HPJ.test.local

< Previous

Next >

Configure

Cancel

AD CS Configuration

Setup Type

Credentials

Role Services

Setup Type

CA Type

Private Key

Cryptography

CA Name

Validity Period

Certificate Database

Confirmation

Progress

Results

Specify the setup type of the CA

Enterprise certification authorities (CAs) can use Active Directory Domain Services (AD DS) to simplify the management of certificates. Standalone CAs do not use AD DS to issue or manage certificates.

☒ Enterprise CA
 Enterprise CAs must be domain members and are typically online to issue certificates or certificate policies.

☐ Standalone CA
 Standalone CAs can be members or a workgroup or domain. Standalone CAs do not require AD DS and can be used without a network connection (offline).

[More about Setup Type](#)

DESTINATION SERVER


WIN-U92CLHC2HPJ.test.local

< Previous

Next >

Configure

Cancel


AD CS Configuration

DESTINATION SERVER
WIN-U92CLHC2HPJ.test.local

CA Type

Credentials

Role Services

Setup Type

CA Type

Private Key

Cryptography

CA Name

Validity Period

Certificate Database

Confirmation

Progress

Results

Specify the type of the CA

When you install Active Directory Certificate Services (AD CS), you are creating or extending a public key infrastructure (PKI) hierarchy. A root CA is at the top of the PKI hierarchy and issues its own self-signed certificate. A subordinate CA receives a certificate from the CA above it in the PKI hierarchy.

☒ Root CA
Root CAs are the first and may be the only CAs configured in a PKI hierarchy.

☐ Subordinate CA
Subordinate CAs require an established PKI hierarchy and are authorized to issue certificates by the CA above them in the hierarchy.


[More about CA Type](#)

< Previous

Next >

Configure

Cancel


AD CS Configuration

DESTINATION SERVER
WIN-U92CLHC2HPJ.test.local

Private Key

Credentials

Role Services

Setup Type

CA Type

Private Key

Cryptography

CA Name

Validity Period

Certificate Database

Confirmation

Progress

Results

Specify the type of the private key

To generate and issue certificates to clients, a certification authority (CA) must have a private key.

☒ Create a new private key
Use this option if you do not have a private key or want to create a new private key.

☐ Use existing private key
Use this option to ensure continuity with previously issued certificates when reinstalling a CA.

☐ Select a certificate and use its associated private key
Select this option if you have an existing certificate on this computer or if you want to import a certificate and use its associated private key.

☐ Select an existing private key on this computer
Select this option if you have retained private keys from a previous installation or want to use a private key from an alternate source.

[More about Private Key](#)

< Previous

Next >

Configure

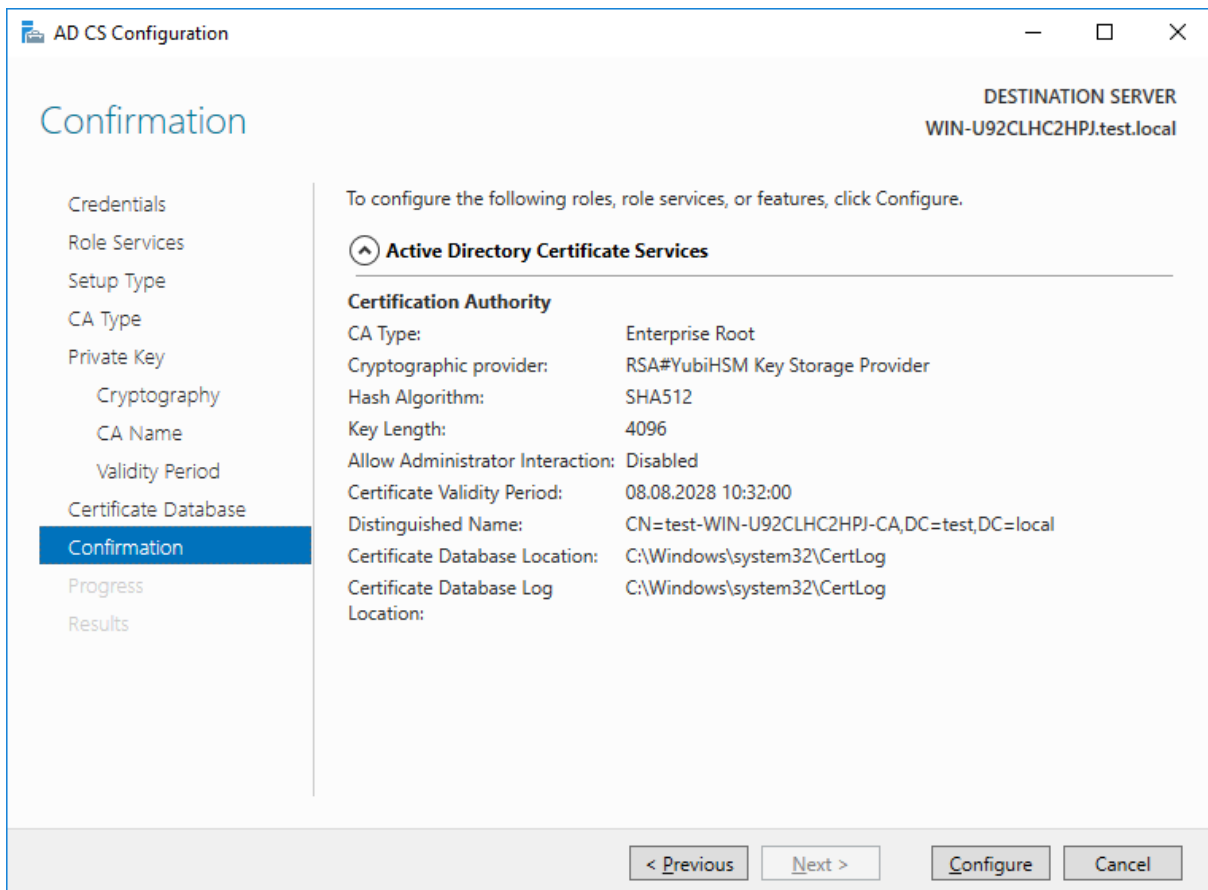
Cancel

Page 43 of 50

The screenshot shows the 'AD CS Configuration' window with the 'Cryptography for CA' step selected in the left-hand navigation pane. The main area is titled 'Specify the cryptographic options'. It contains two dropdown menus: 'Select a cryptographic provider:' set to 'RSA#YubiHSM Key Storage Provider' and 'Key length:' set to '4096'. Below these is another dropdown menu 'Select the hash algorithm for signing certificates issued by this CA:' with 'SHA512' selected. A checkbox labeled 'Allow administrator interaction when the private key is accessed by the CA.' is currently unchecked. At the bottom right, there are four buttons: '< Previous', 'Next >', 'Configure', and 'Cancel'. A link 'More about Cryptography' is located at the bottom left of the main content area.

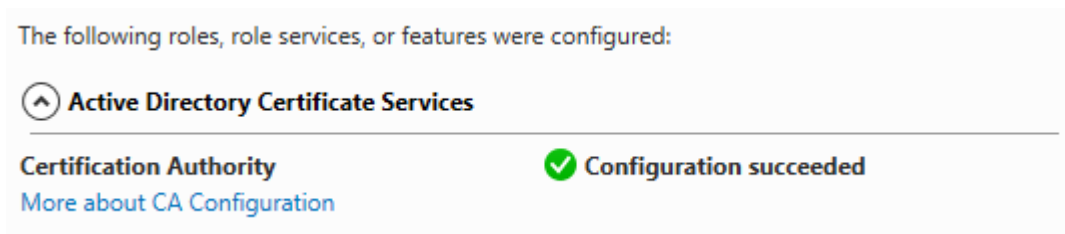
Select RSA#YubiHSM Key Storage Provider from the list displayed. This indicates that the root key should be generated on the YubiHSM.

Proceed with the Wizard.



In the Confirmation page, the important detail is that the YubiHSM Key Storage Provider is being used to store the CA private key. Click Configure.

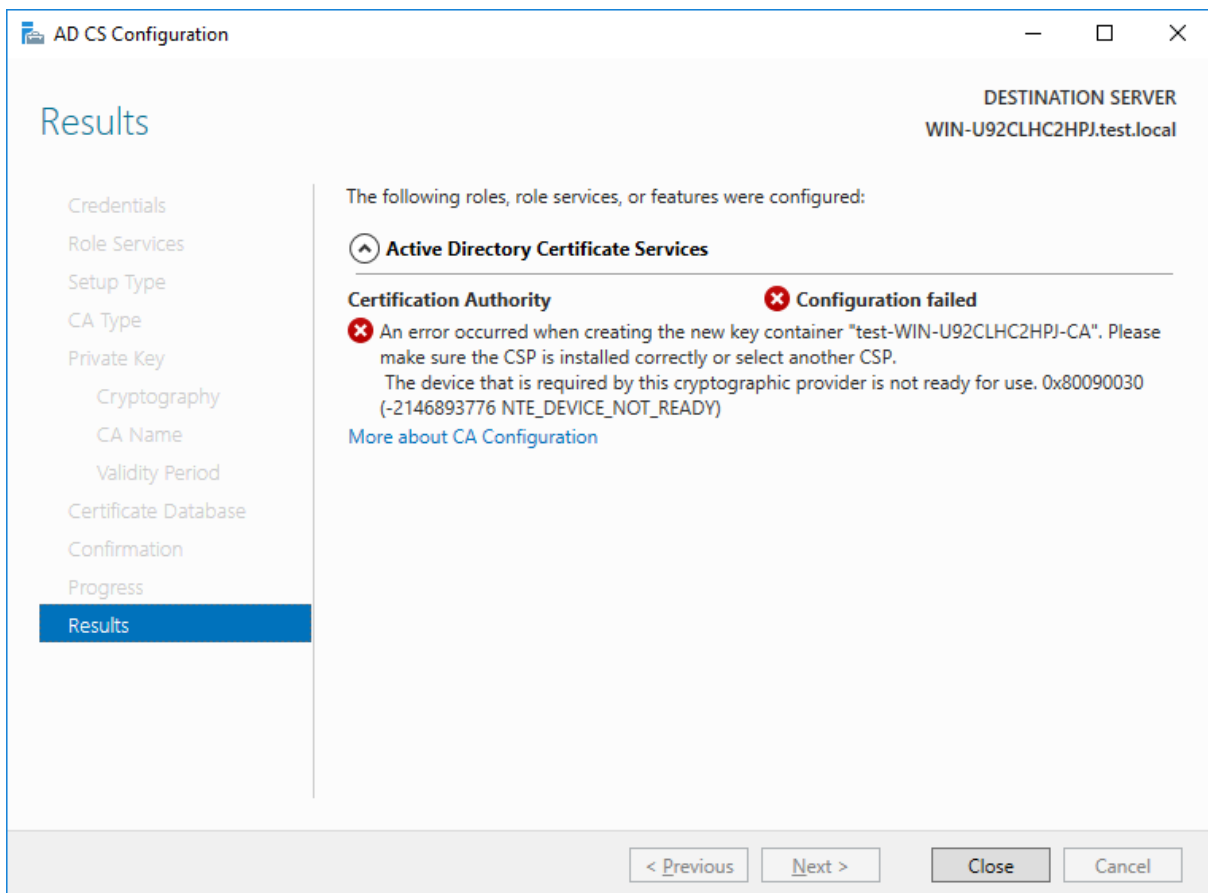
Now you should see “Configuration succeeded” in the Results page.



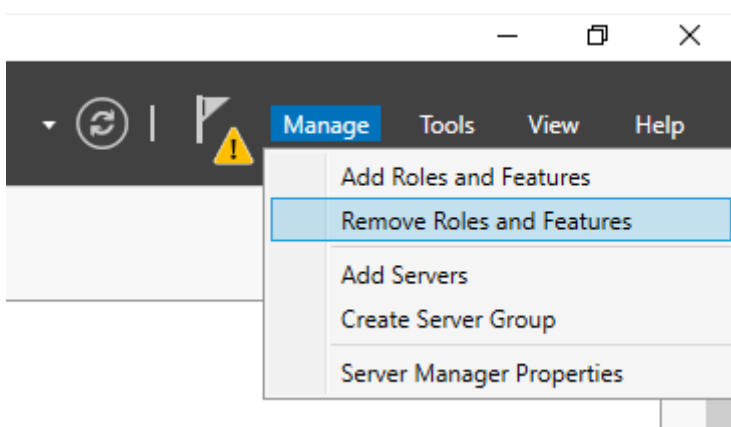
The Active Directory Certificate Services are now ready for use.

9 Troubleshooting

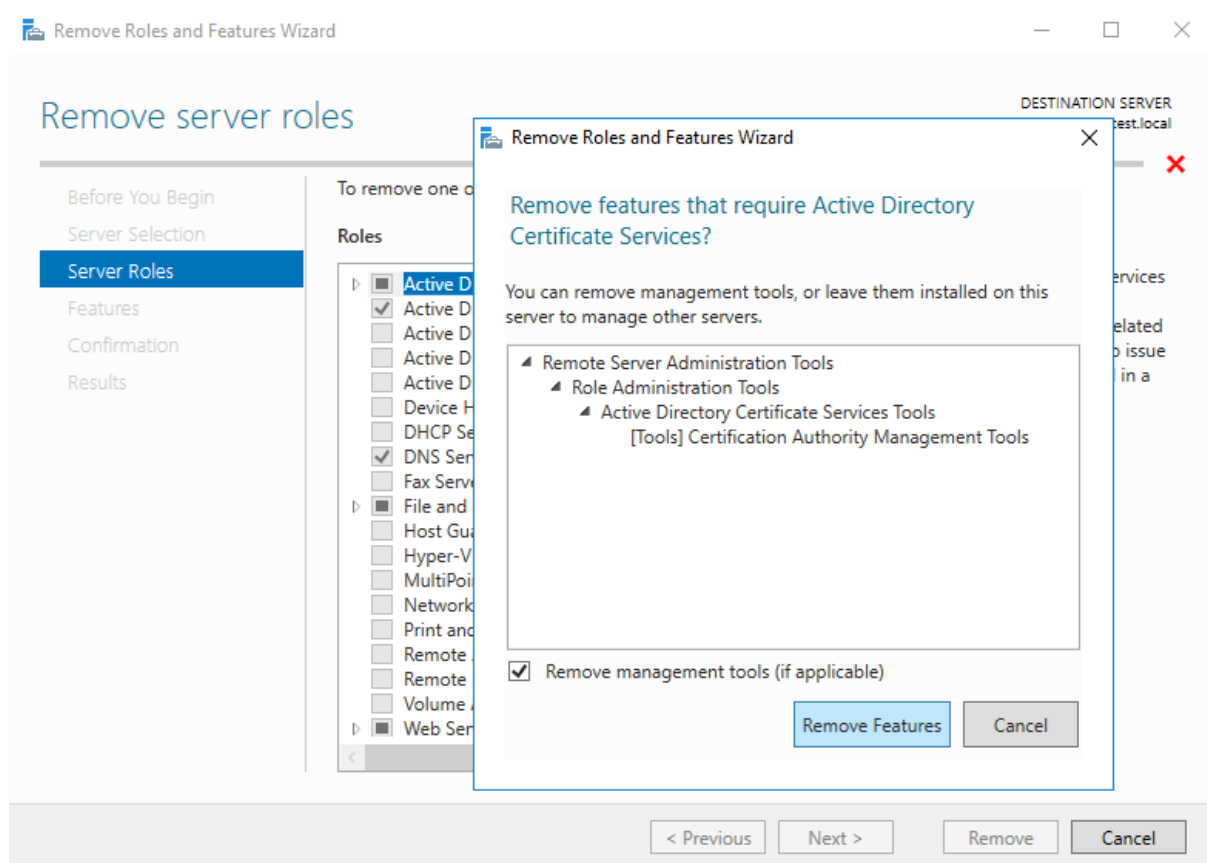
9.1 Active Directory Certificate Services



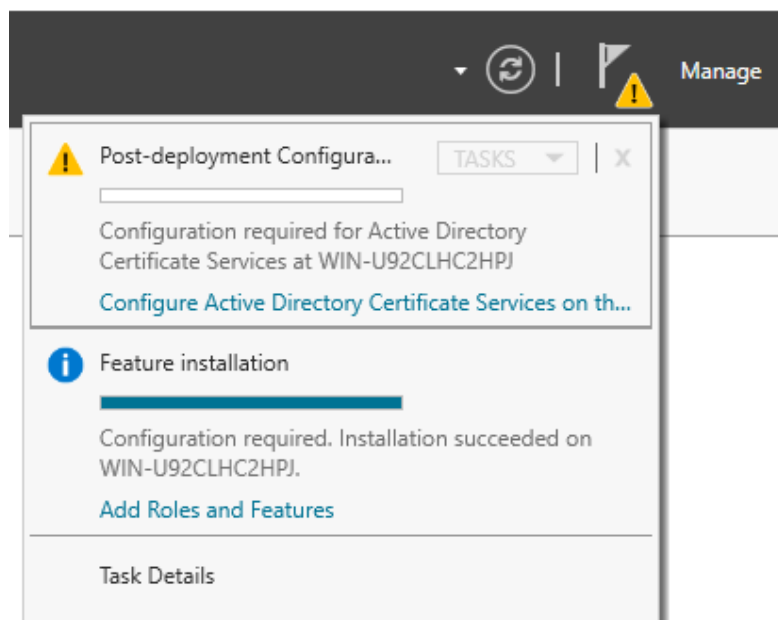
If you don't see "Configuration succeeded" but instead get the error "The device that is required by this cryptographic provider is not ready for use.", you can try this:



Remove the Active Directory Certificate Services and install them again like shown before.

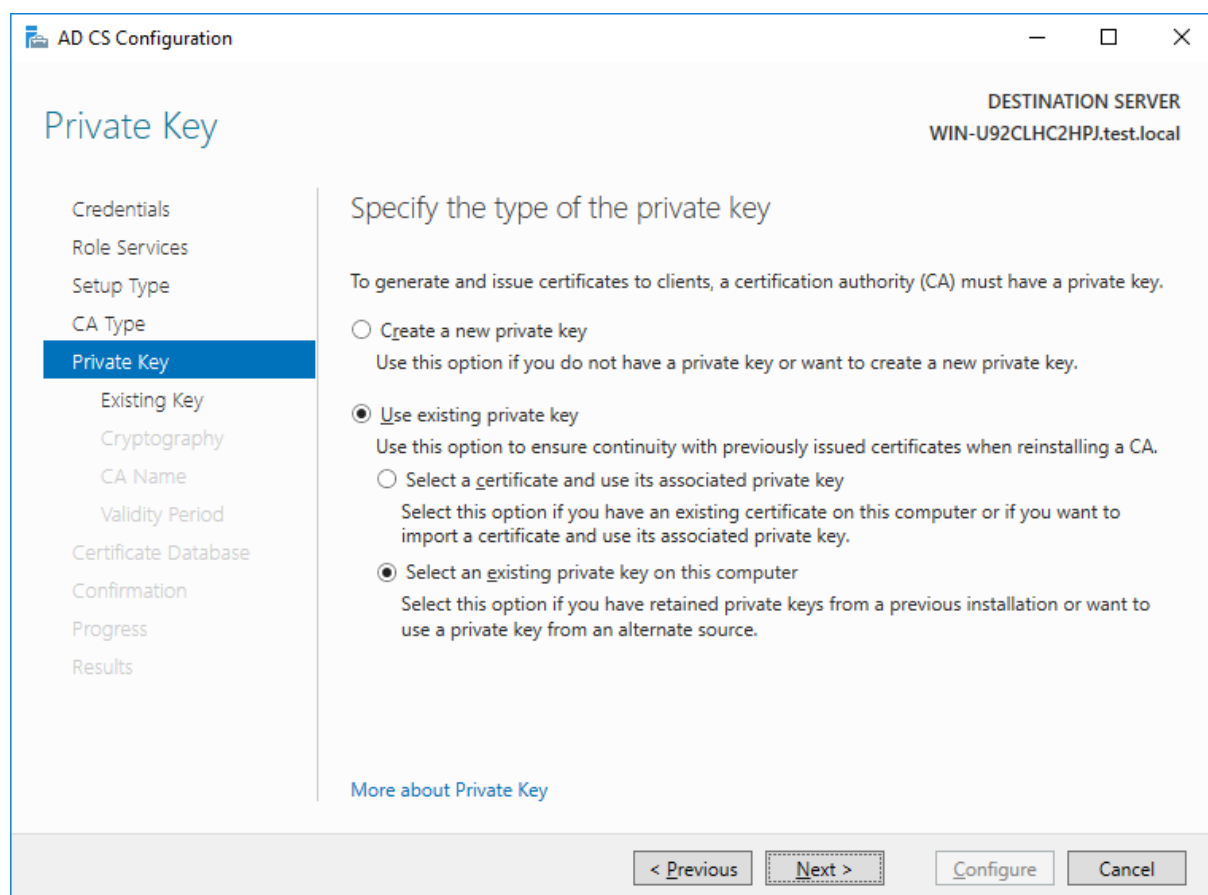


After reinstalling the Active Directory Certificate Services, start the configuration Wizard again.



Proceed the Wizard as before but in the "Private Key" page, select "Use existing private key" instead of creating a new one. (It is possible the key was already created before but the Wizard still reported "Configuration failed".)

Choose “Select an existing private key on this computer”.



AD CS Configuration

DESTINATION SERVER
WIN-U92CLHC2HPJ.test.local

Private Key

Credentials
Role Services
Setup Type
CA Type
Private Key
Existing Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results

Specify the type of the private key

To generate and issue certificates to clients, a certification authority (CA) must have a private key.

☐ Create a new private key
Use this option if you do not have a private key or want to create a new private key.

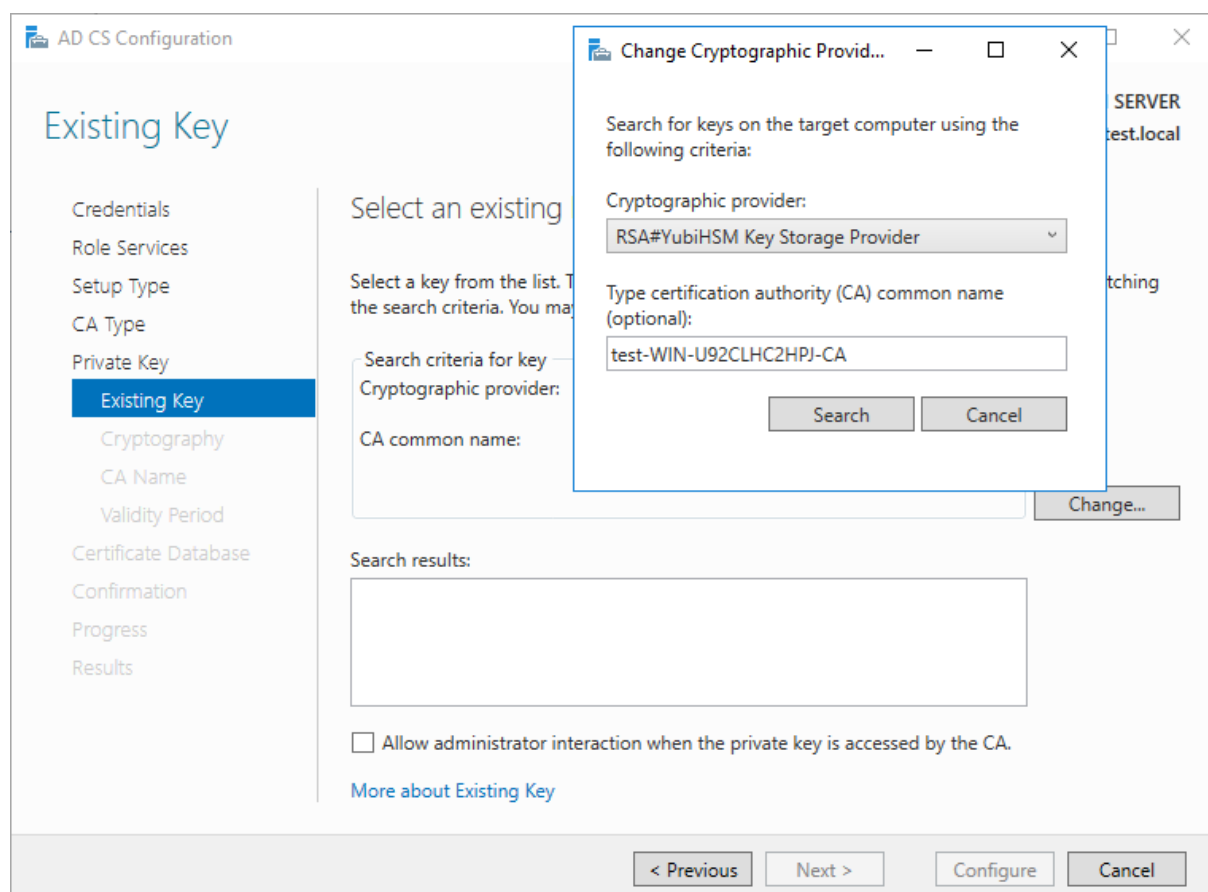
☒ Use existing private key
Use this option to ensure continuity with previously issued certificates when reinstalling a CA.

☐ Select a certificate and use its associated private key
Select this option if you have an existing certificate on this computer or if you want to import a certificate and use its associated private key.

☒ Select an existing private key on this computer
Select this option if you have retained private keys from a previous installation or want to use a private key from an alternate source.

[More about Private Key](#)

< Previous Next > Configure Cancel



AD CS Configuration

SERVER
test.local

Existing Key

Credentials
Role Services
Setup Type
CA Type
Private Key
Existing Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results

Select an existing

Select a key from the list. The search criteria. You may specify the search criteria for key.

Search criteria for key
Cryptographic provider:
CA common name:

Change Cryptographic Provider...

Search for keys on the target computer using the following criteria:

Cryptographic provider:
RSA#YubiHSM Key Storage Provider

Type certification authority (CA) common name (optional):
test-WIN-U92CLHC2HPJ-CA

Search Cancel

Change...

Search results:

☐ Allow administrator interaction when the private key is accessed by the CA.

[More about Existing Key](#)

< Previous Next > Configure Cancel

In the “Existing Key” page select “Change...” and choose the YubiHSM Key Storage Provider.

Click on Search.

AD CS Configuration

Existing Key

DESTINATION SERVER
WIN-U92CLHC2HPJ.test.local

Credentials
Role Services
Setup Type
CA Type
Private Key
Existing Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results

Select an existing key

Select a key from the list. The listed keys are the keys available on the target computer matching the search criteria. You may change the search criteria.

Search criteria for key

Cryptographic provider: RSA#YubiHSM Key Storage Provider

CA common name: test-WIN-U92CLHC2HPJ-CA

[Change...](#)

Search results:

test-WIN-U92CLHC2HPJ-CA

☐ Allow administrator interaction when the private key is accessed by the CA.

[More about Existing Key](#)

< Previous Next > Configure Cancel

If you see anything in the Search results name like [Server name]-CA, then the private key was already created in the first try and you can use this key to complete the Wizard.

Click Next and ensure the YubiHSM Key Storage Provider is selected.

AD CS Configuration

Cryptography for CA

DESTINATION SERVER
WIN-U92CLHC2HPJ.test.local

Credentials
Role Services
Setup Type
CA Type
Private Key
Existing Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results

Specify the cryptographic options

Select a hash algorithm for signing certificates issued by this certification authority (CA).

Cryptographic provider:
RSA#YubiHSM Key Storage Provider

Hash algorithm:
SHA256
SHA384
SHA512
SHA1

[More about Cryptography](#)

< Previous Next > Configure Cancel

Proceed with the Wizard, now the Configuration should succeed.

The following roles, role services, or features were configured:

⬆ **Active Directory Certificate Services**

Certification Authority ✔ **Configuration succeeded**

[More about CA Configuration](#)