

iQSol HSA

Hardware Security Appliance

HSA v5.2, 9. January 2025

Index

1	Installation.....	9
1.1	Requirements.....	9
1.1.1	Required Ports	9
1.2	HSA Quick Start Guide	10
1.2.1	How to access the HSA.....	10
1.2.2	Recommended PuTTY settings.....	10
1.2.3	Network settings.....	10
1.3	ISO Image	11
1.4	User Manual	11
2	Setup Wizard.....	12
2.1	Starting the Wizard.....	12
2.2	Change keymap	12
2.3	License.....	12
2.4	Hostname.....	13
2.5	Setting the correct time	13
2.6	Changing NTP	13
2.7	Changing password.....	14
2.8	Wizard completed.....	14
3	Main menu	15
4	Info menu.....	17
4.1	manual.....	17
4.2	status	17
4.3	license	17
4.3.1	upload.....	18
4.3.2	copy/paste.....	18
5	Network menu.....	19
5.1	hostname.....	19
5.2	interface	19

5.2.1	Edit interface	20
5.3	Gateway.....	20
5.4	NTP	20
5.5	DNS.....	20
5.6	searchDomain.....	21
5.7	addRoute	21
5.8	listRoute	21
5.9	show.....	21
5.10	apply.....	21
6	YubiHSM menu.....	22
6.1	info.....	22
6.2	listenIP	22
6.3	cert	22
6.4	Setup a new YubiHSM.....	23
6.4.1	Creating a Wrapkey	23
6.4.2	Creating the Admin Authentication Key	25
6.5	Authentication Key	27
6.5.1	Authentication Key ID	27
6.5.2	Authentication Key label.....	28
6.5.3	Authentication Key Domain.....	29
6.5.4	Authentication Key Capabilities.....	29
6.5.5	Choose a password	30
6.5.6	Authentication Key stored on the YubiHSM	30
6.6	import	30
6.7	create.....	31
6.7.1	Asymmetric Key ID	31
6.7.2	Asymmetric Key label.....	31
6.7.3	Authentication Key for Asymmetric Key.....	32
6.7.4	Asymmetric Key stored on the YubiHSM.....	32

6.8	backup.....	33
6.9	tools.....	33
6.9.1	deviceinfo	33
6.9.2	objectInfo	33
6.9.3	removeKey	33
6.9.4	listObjects	33
6.9.5	listBackup.....	33
6.9.6	domainOverview.....	33
6.9.7	shell.....	33
6.10	connector.....	34
6.10.1	restartCon.....	34
6.10.2	start.....	34
6.10.3	stop.....	34
6.10.4	rmSN.....	34
6.10.5	writeSN.....	34
6.10.6	manSN	35
6.10.7	allowIP	35
6.10.8	listIP.....	35
7	HSA menu.....	36
7.1	users	36
7.2	Time.....	36
7.2.1	View.....	37
7.2.2	Time.....	37
7.2.3	Date.....	37
7.2.4	Timezone.....	38
7.3	keymap.....	38
7.4	update.....	39
7.5	backup.....	39
7.6	restore.....	39

7.7	CAcert.....	39
7.8	downloadCert.....	39
7.9	mail.....	40
7.10	restartNginx.....	40
7.11	wizard.....	40
7.12	color.....	40
7.13	reboot.....	41
7.14	shutdown.....	41
8	ACME menu.....	42
8.1	show.....	42
8.2	setup.....	42
8.3	listenIP.....	43
8.4	cert.....	43
8.5	configure.....	44
8.5.1	Mode – mswcce.....	44
8.5.2	Mode – acme-ca.....	46
8.6	start.....	46
8.7	stop.....	46
8.8	log.....	46
8.9	nginx.....	47
8.10	destroy.....	47
9	EST Menu.....	48
9.1	show.....	48
9.2	setup.....	48
9.3	listenIP.....	49
9.4	cert.....	49
9.5	configure.....	50
9.6	auth.....	51
9.7	start.....	51

9.8 stop.....	51
9.9 log.....	51
9.10 nginx.....	51
9.11 destroy	51
10 Cluster menu	52
10.1 clusterWizard.....	52
10.2 show.....	52
10.3 addIP.....	52
10.4 deleteIP.....	52
10.5 createClusterSeed	53
10.6 importClusterSeed.....	53
10.7 disable.....	53
10.8 enable.....	53
10.9 destroy	53
11 Logging menu	54
11.1 Syslog.....	54
11.1.1 local.....	54
11.1.2 remote.....	54
11.1.3 server.....	54
11.1.4 TLS.....	54
11.1.5 display.....	55
11.2 SNMP.....	55
11.2.1 enable/disable.....	55
11.2.2 OID	55
11.2.3 port.....	55
11.2.4 sysLocation	56
11.2.5 sysContact.....	56
11.2.6 user.....	56
11.2.7 listUser	56

12	YubiHSM setup on a Windows CA	57
12.1	Installing the connector certificate	57
12.2	Installing the YubiHSM Key Storage Provider	59
12.3	New CA Server	62
12.3.1	Add the CA Role	62
12.3.2	Configure Active Directory Certificate Services	63
12.4	Migrate existing (root) CA certificate	68
12.4.1	Export certificate to .pfx file	68
12.4.2	Import private key to YubiHSM	74
12.4.3	Decommission old Key Storage Provider	76
12.4.4	Import certificate on CA	76
12.4.5	Registry Editor	76
12.4.6	Repair the Keystorage:	77
13	YubiHSM setup on a Linux CA	78
13.1	Linux CA Prerequisites	78
13.2	Configuration on the YubiHSM	78
13.2.1	YubiHSM default setup on the HSA	78
13.2.2	Generate a new authentication key	78
13.2.3	Generate an Asymmetric Key	79
13.3	Configuration on EJBCA	79
13.4	Configuration on other CAs	79
14	Setup CA for ACME/EST	80
14.1	Creating Users for Authentication with the CA	80
14.2	Creating a certificate template to issue	81
14.3	Exporting the CA bundle	83
14.4	Finishing touches	83
15	Let's Encrypt Mode for ACME	83
16	YubiHSM Troubleshooting	84
16.1	Active Directory Certificate Services	84

17 ACME/EST Troubleshooting.....	90
----------------------------------	----

1 Installation

1.1 Requirements

1.1.1 Required Ports

Following ports are required:

Function	Direction			Port
HSA outgoing communication				
ACME – MS-WCCE	HSA	⇒	Windows CA	445/TCP
EST – Windows CA	HSA	⇒	Windows CA	445/TCP
HSA incoming communication				
HSA Cluster	HSA	⇒	HSA	22/TCP 2224/TCP 5404/TCP 5405/TCP
YubiHSM	Windows CA	⇒	HSA	443/TCP
ACME Protokoll	Requesting Server	⇒	HSA	443/TCP
EST Protokoll	Requesting Server	⇒	HSA	9443/TCP
User configuration	SSH/HTTPS Client	⇒	HSA	22/TCP 8443/TCP

1.2 HSA Quick Start Guide

1.2.1 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 an USB keyboard or the Serial Port.

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

1.2.2 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".

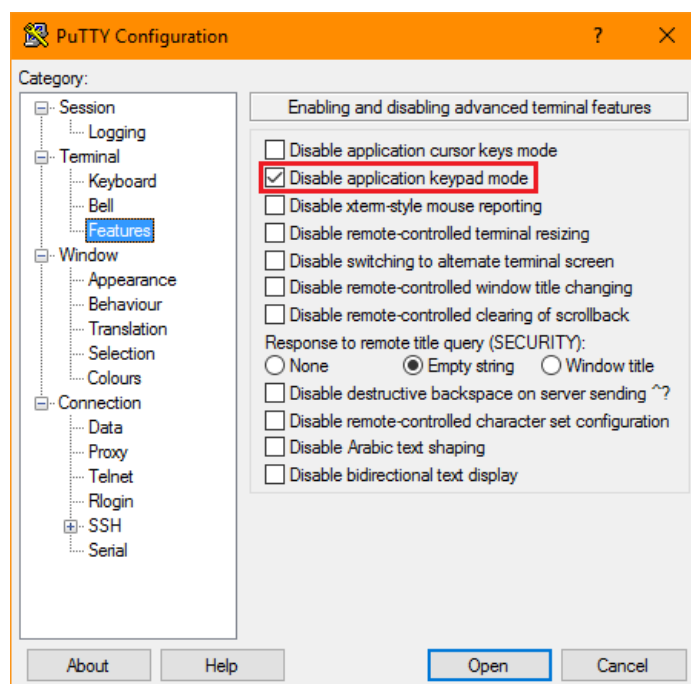
It is also recommended to change the window and text size for readability.

"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".



1.2.3 Network settings

After the first login the wizard starts, to configure the most important system settings.

Afterwards you can change the IP address in the network submenu.

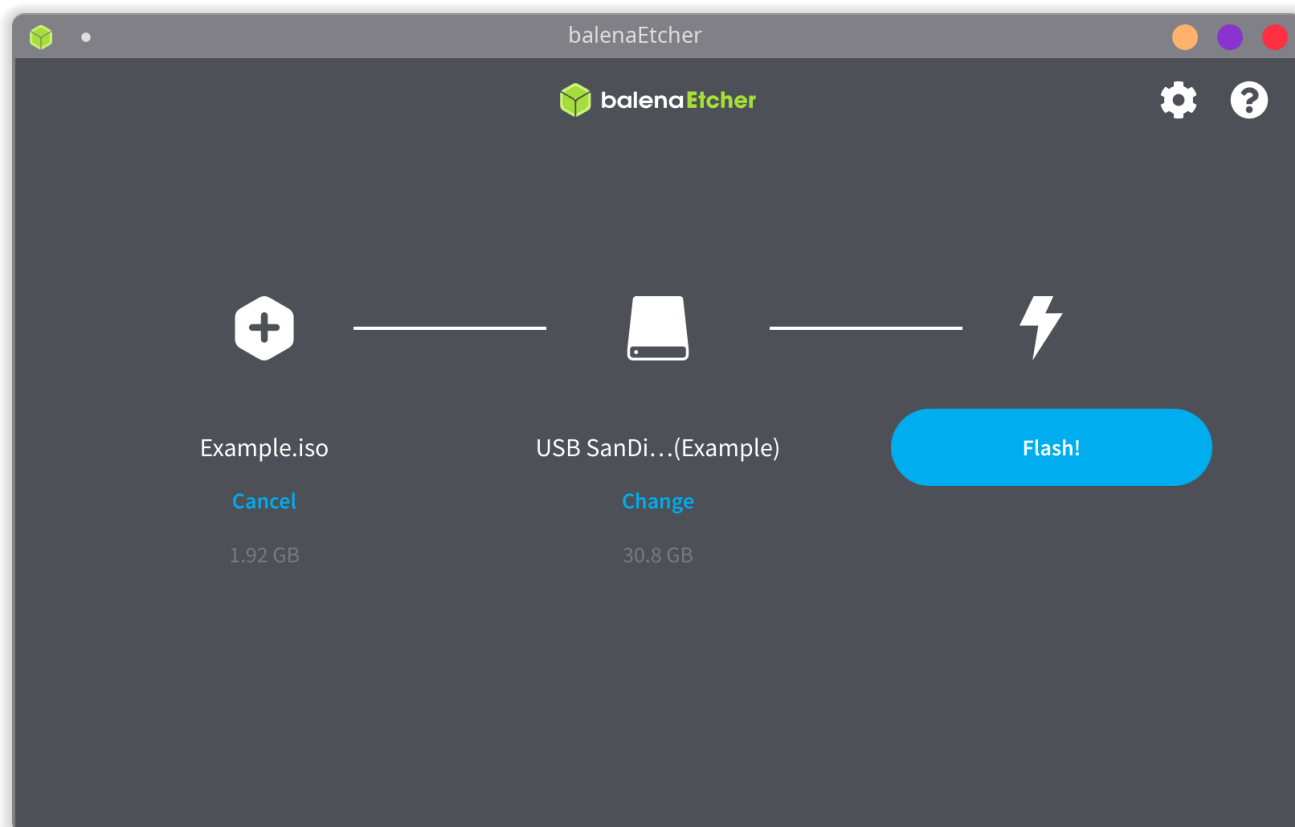
Change both the IP via interface > eth0 > changeIP and the Gateway (directly in the network menu as the default gateway is set system wide, and not per interface).

The changes will only take effect after you select "apply" in the network menu, or the system is rebooted.

1.3 ISO Image

The ISO is a hybrid ISO with UEFI and BIOS support. It can be booted in a VM in UEFI or BIOS mode. It also contains the required partition information for USB drives and can be copied directly to a USB flash drive.

A simple tool to copy the ISO to an USB disk is balenaEtcher.



If you are familiar with the Linux CLI, you can also use a command like the following:
dd bs=4M if=path/to/example.iso of=/dev/sdx conv=fsync oflag=direct status=progress

Rufus is also suitable as an alternative GUI tool.

We recommend that you set your hardware to UEFI mode before installation.

1.4 User Manual



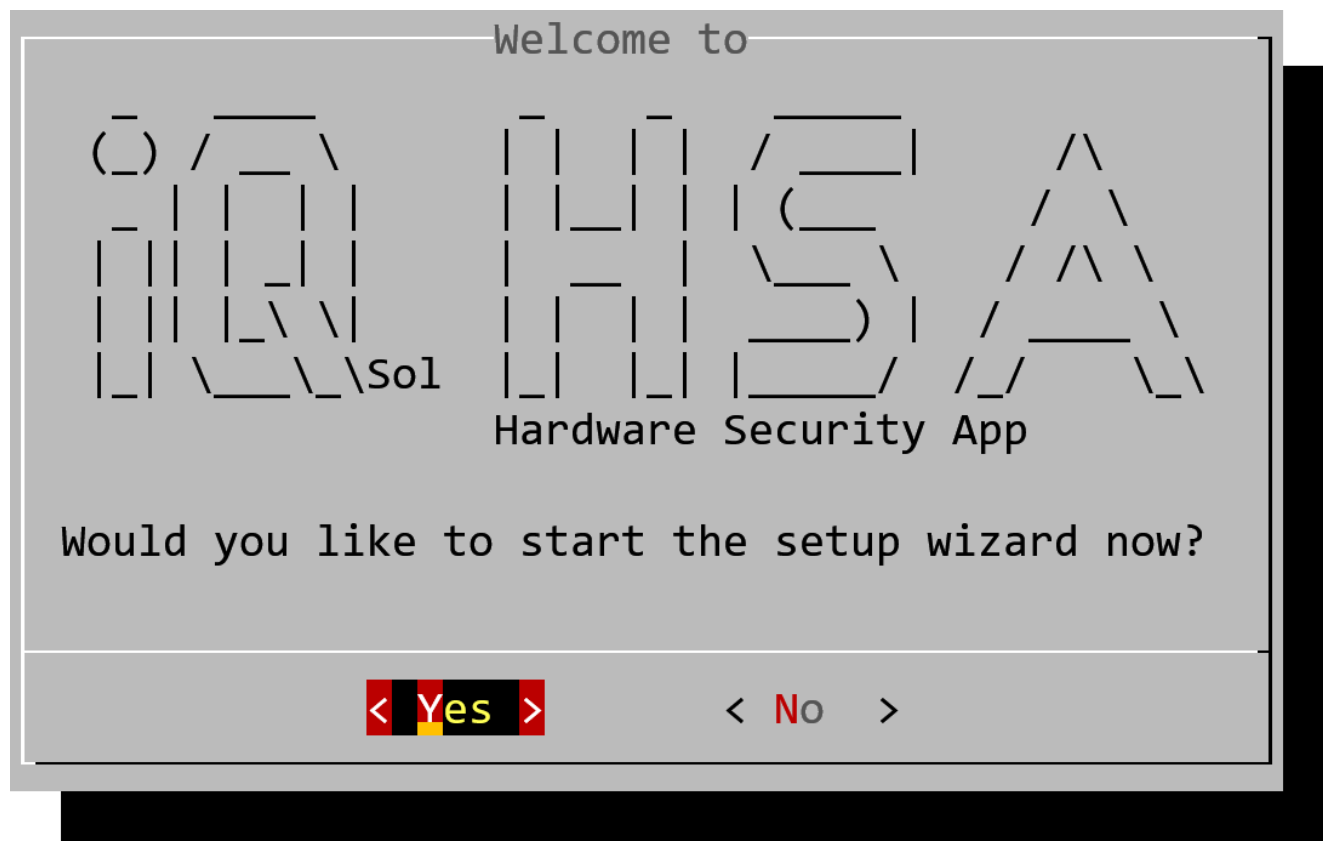
An always up-to-date user manual can be found here:

<https://asf.anlx.cloud/index.php/s/NNHq6S4XzGcb46r?path=%2FHARDWARE%20SECURITY%20APPLIANCE>

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.

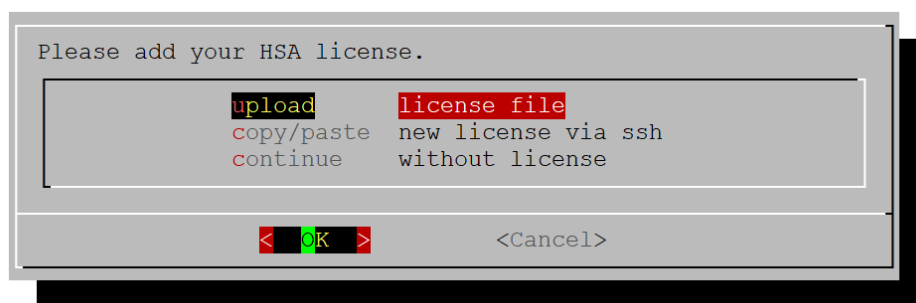
Select “Yes” to start the wizard or “No” if you already know all the important steps and want to select them manually in the menu.

2.2 Change keymap

First you can change the keymap of your keyboard.

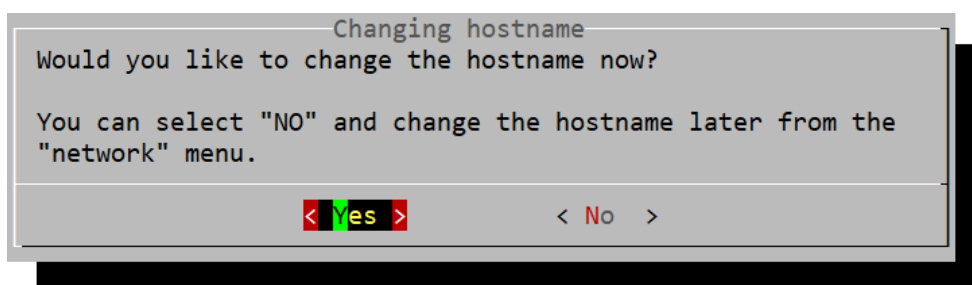
2.3 License

Next, you can select how or if you want to add a license.



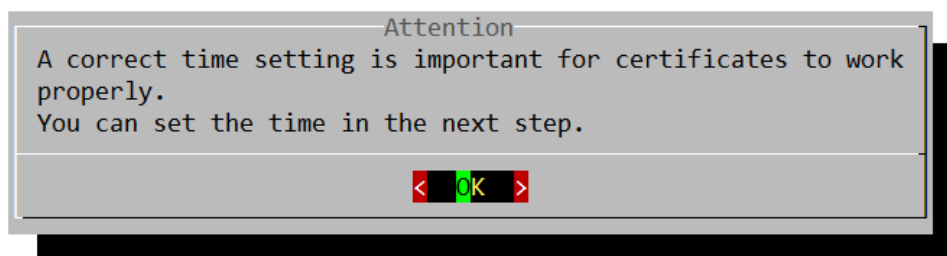
If you want to add a license later, you can do so in the [Info menu](#).

2.4 Hostname



If you are configuring a cluster, you must change the hostname now, otherwise conflicts may occur when you create the cluster. This hostname also needs to be listed on your DNS server.

2.5 Setting the correct time



In the following screens you can configure the system time.

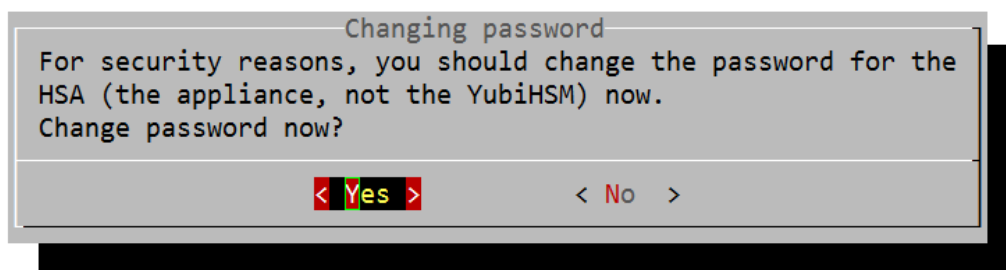
- Timezone: [HSA menu](#) > [Time](#) > [Timezone](#)
- Date: [HSA menu](#) > [Time](#) > [Date](#)
- Time: [HSA menu](#) > [Time](#) > [Time](#)

2.6 Changing NTP

Now you can enter a NTP server for automatic time updates.

You can also do this later in: [Network menu](#) > [NTP](#)

2.7 Changing password



This is important to ensure that the HSA is secure. Choose a secure password!

First change the password 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 has unrestricted rights on the HSA.

The default password is: deviceadmin

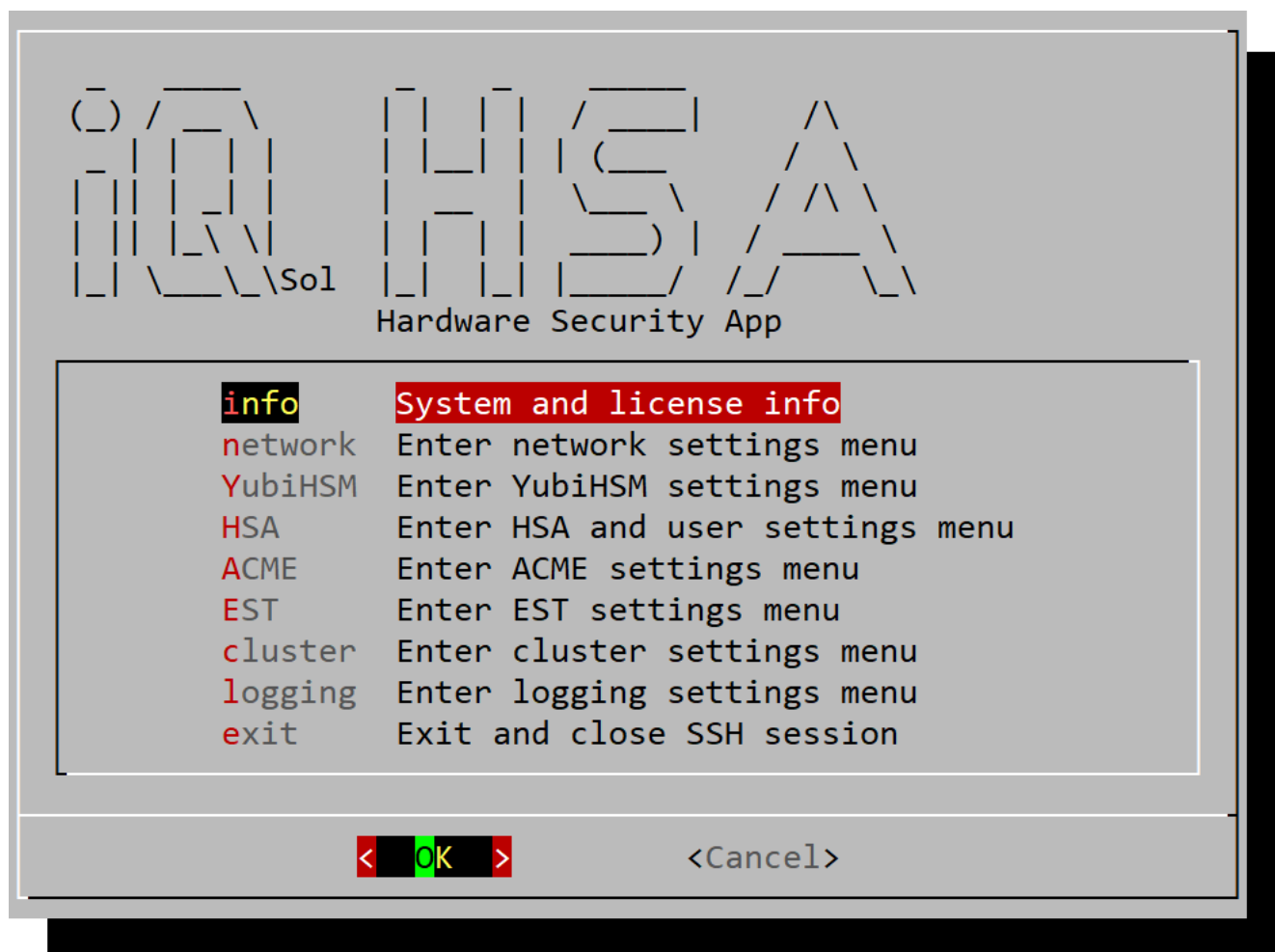
Note: There are separate passwords for the YubiHSM module. These are not affected by these settings.

2.8 Wizard completed



The next time you log in, the Wizard will not start. Instead, the main menu will be displayed.

3 Main menu



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

- “info” views some basic information about the device and software and has the option to download the HSA User Manual: [Info menu](#)
- In the “network” submenu you can find all network related settings: [Network menu](#)
- In the “YubiHSM” submenu you can find settings related to the YubiHSM module: [YubiHSM menu](#)
- “HSA” contains settings for the HSA Box itself: [HSA menu](#)
- In “ACME” you can configure ACME settings: [ACME menu](#)
- In “EST” you can configure EST settings: [EST menu](#)
- In “cluster” you can change all cluster related settings: [Cluster menu](#)
- In “logging” you can change logging related settings: [Logging menu](#)

The menu offers 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 Info menu

Provides information about the HSA:

- Hostname
- HSA version

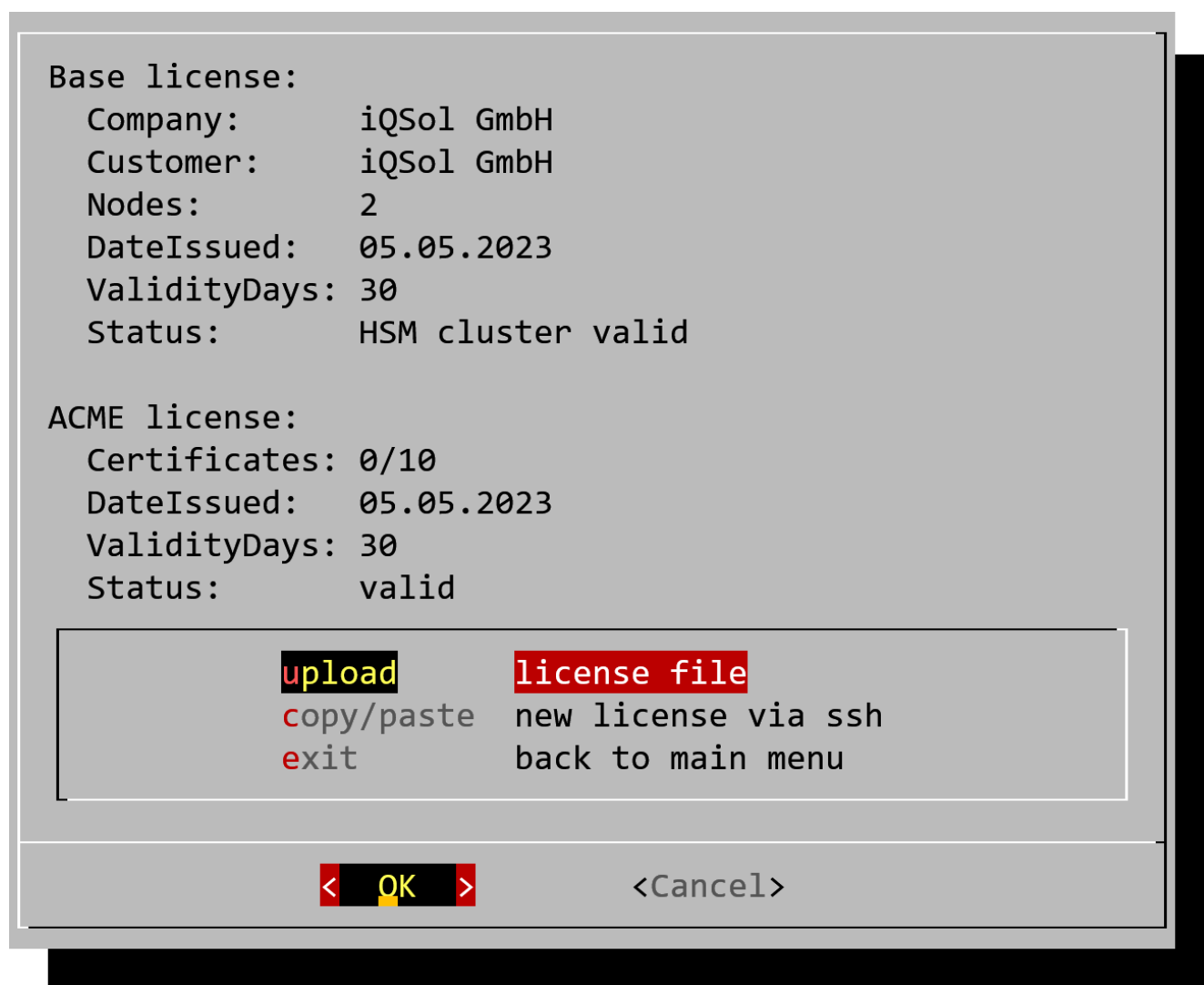
4.1 manual

Starts a wizard for downloading the user manual.

4.2 status

Displays the status of the services on the HSA.

4.3 license



Provides information about your current base, HSM and ACME license.

4.3.1 upload

Upload a license via scp or ftp.

4.3.2 copy/paste

If you selected “copy/paste”, copy your license and then paste it with right click into the nano window. After that, press ctrl + s to save and then you can exit with ctrl + x.

```

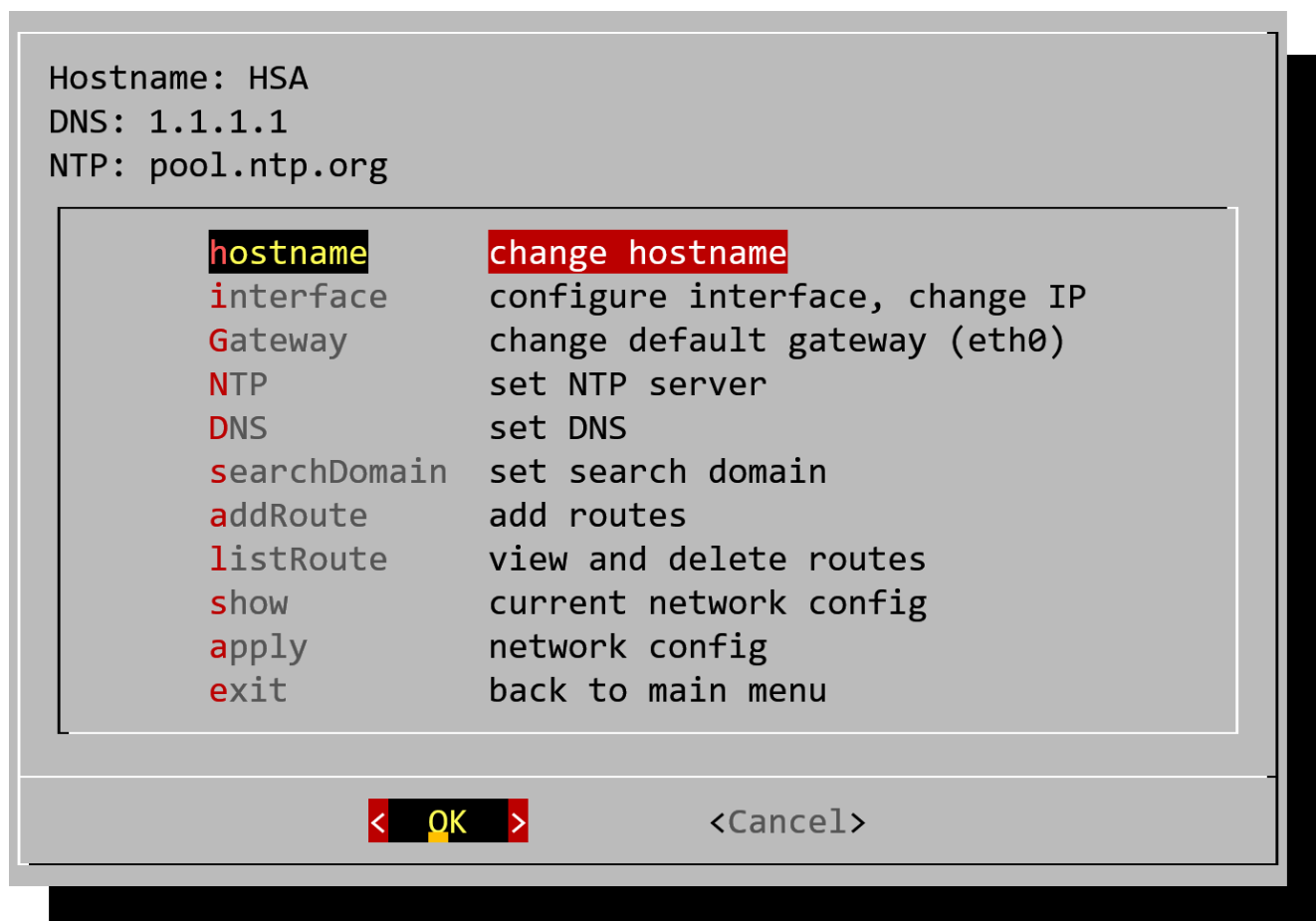
GNU nano 5.4 /home/deviceadmin/imported.hsalic Modified
----- BEGIN LICENSE -----
Product: HSA
Version: 4.0
Company: iQSol GmbH
Customer: iQSol GmbH
Nodes: HardwareSecurityApp: 1
DateIssued: 26/04/2022
ValidityDays: 30
MaintenanceDays: 30

LICDATA-r1WxLKEuVwbvp01MJKqalZcGIx1moRD2rSWvMzuTMyECFSqcGmuYZJSerUE1M
nwODMJ55F0c1MyInMTAHD1jiAHV2IR1cZmWZHI0uFwuZGR5CpHcFnJI6D1jiZSIAPmAdr
...
J5cqQxkJHAKf1WZoK0xFlgaraWnpJyPExgWAQMLAmSbHRSuF0WSBTgEKP9pY050CG0vYP
4ISyDExIMomD0qS00Z3cyJwEOG1MhZUMSpycyGRcAGxAWHz9nGxI3E3LeLy0EL2k6KP9d
0AmN4MJAvZTZkVa0====
----- END LICENSE -----

^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^J Justify
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^T Execute

```

5 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 settings.

5.1 hostname

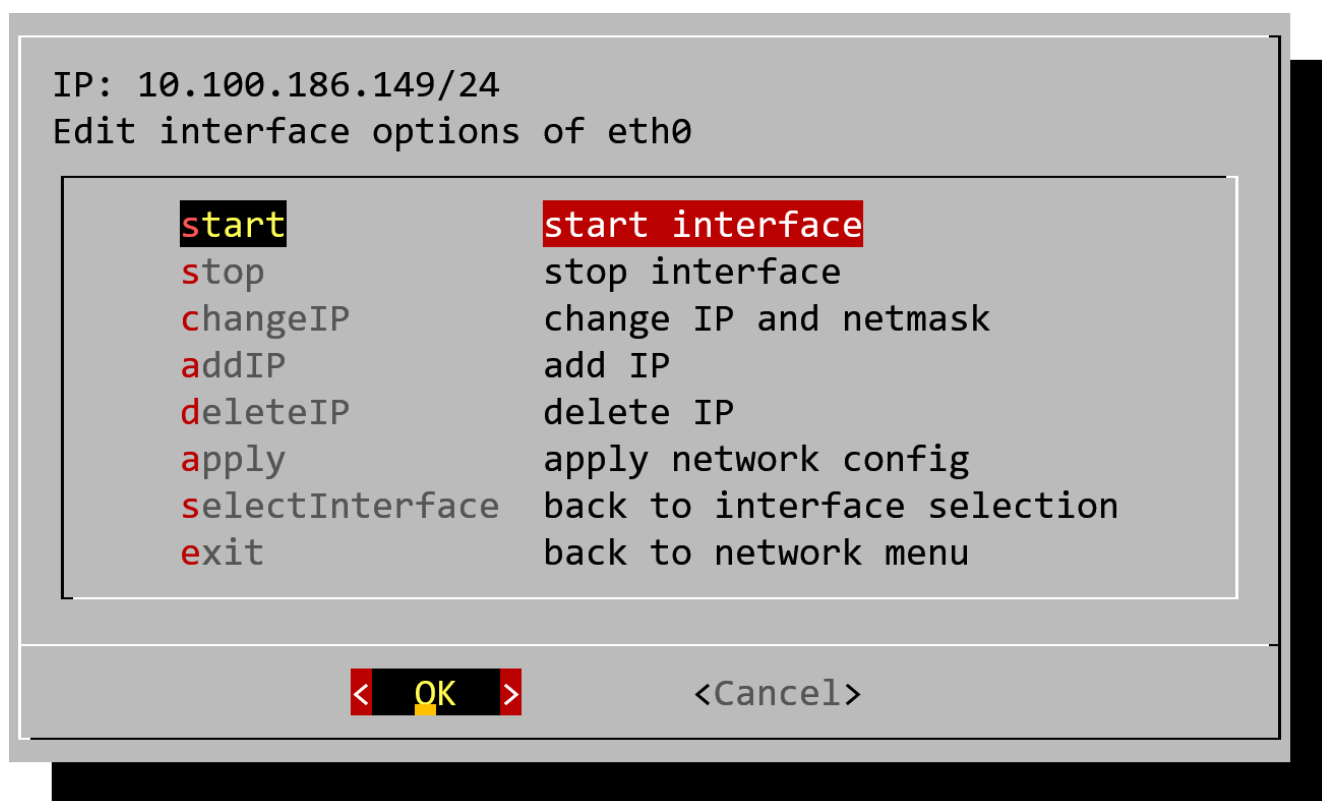
You can change the system host name to make it easier to identify on the network.

5.2 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.

5.2.1 Edit interface



- “start” and “stop” should only be used if you are connected via HDMI and a USB keyboard. Otherwise, you will lose the connection to the HSA.
- With “changeIP” you can select an IP which you want to change.
- With “addIP” you can add an additional IP to the interface. So, you can make different services work on different IPs.
- With “deleteIP” you can delete IPs no longer needed.

5.3 Gateway

Here you can change the system wide default gateway.

5.4 NTP

You can use an NTP server on the local network.

5.5 DNS

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

5.6 searchDomain

If you use a local domain, you can enter the domain name here, so DNS lookups won't fail for it.

5.7 addRoute

Add routes to the routing table.

5.8 listRoute

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

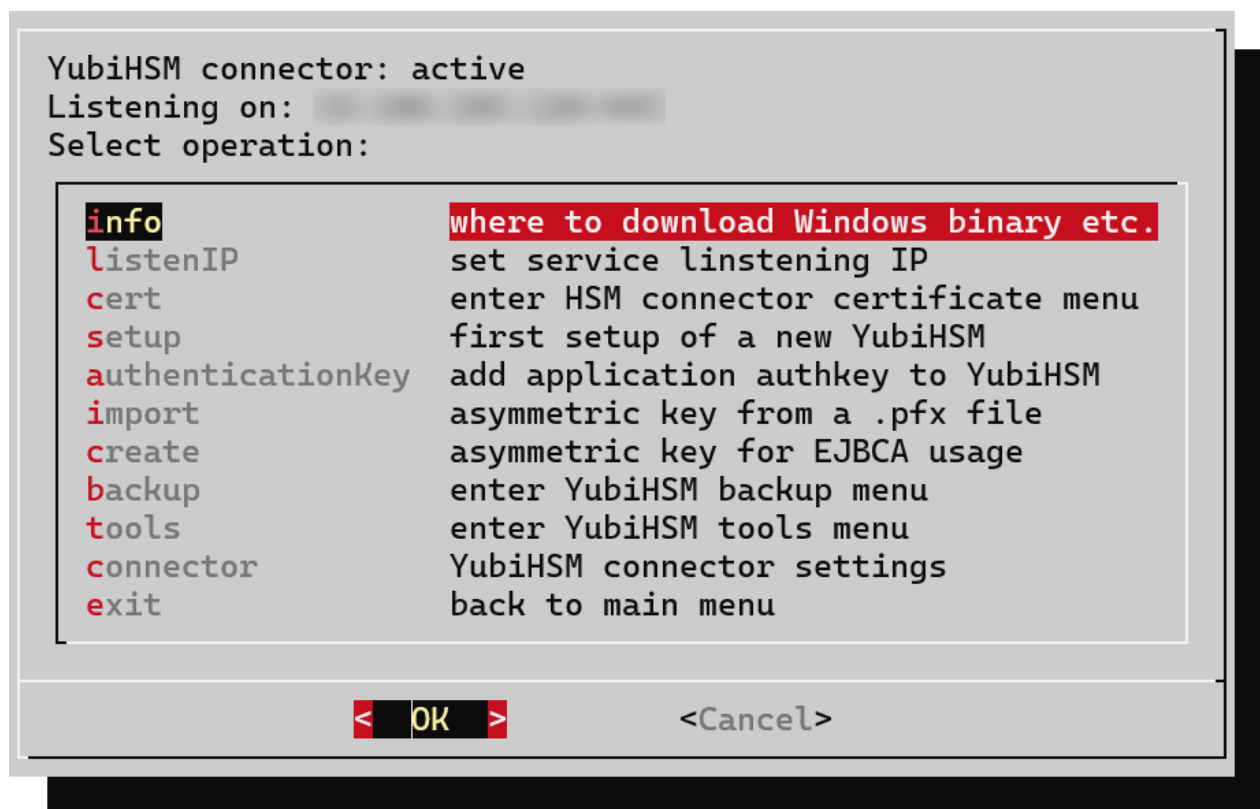
5.9 show

Shows the currently saved network config for verification.

5.10 apply

Applies the currently saved network config, so that changes will take effect.

6 YubiHSM menu



6.1 info

Contains some basic information and useful links about the YubiHSM.

6.2 listenIP



Please ensure that a different IP is used for each of the YubiHSM, ACME and EST service.

Here you can select an IP on which the connector service should listen for incoming connections. Additional IPs can be added via network settings for an interface or if you have a cluster, in the cluster menu.

6.3 cert

Note: The encoding of files created from this menu is PEM. Files uploaded via this menu must also be encoded in PEM.

Go to the connector certificate submenu to manage the public https certificate for the YubiHSM connector.

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

The following options are available:

Create

Create a new self signed certificate.

Import

Import an externally created certificate and private key.

Download

Download the current public certificate.

CSR

Create a certificate signing request to be signed by a CA.

Note: This is not recommended for the YubiHSM connector as the CA will probably need the YubiHSM to sign certificates, and this connection should work independent of it.

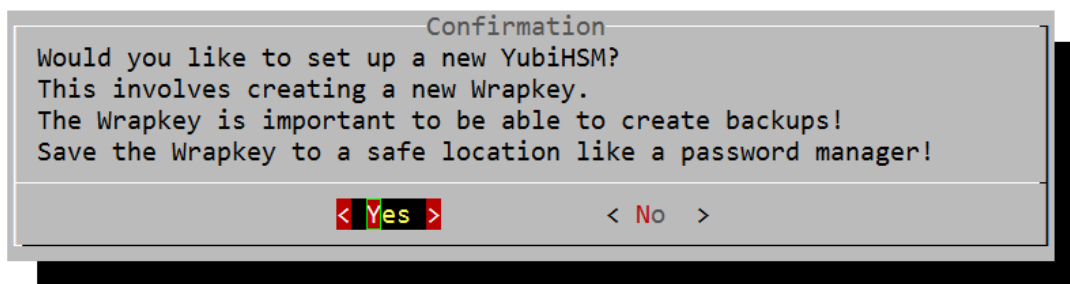
CRT

Import the signed certificate which was created with a CSR.

6.4 Setup a new YubiHSM

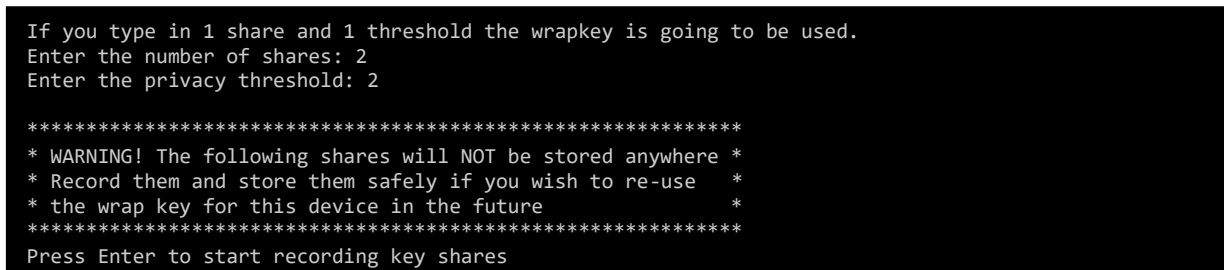
6.4.1 Creating a Wrapkey

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



Select "Yes"

Using key shares



Type in the number of shares and the privacy threshold. If you type in 1 share and 1 threshold the wrapkey will be prompted and used (go down to [Use the plain text wrapkey directly](#))

Note: shares \geq threshold

The shares are the different parts you get to distribute amongst different people so a single person cannot restore the key.

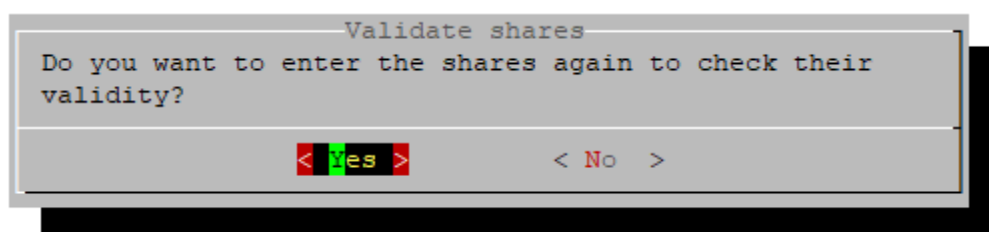
The threshold is the number of shares that may be missing in order for recovery to still be allowed.

Shares will look like this:

```
2-1-8bD1fcNDBSSr602bYnzTze0LDE3eaCB4ebJoLA1b8eTFQrkp5LoMABEI63H16V2jtM0z2w
Have you recorded the key share? (y/n)
```

[threshold]-[current share]-[value]

After you or someone else saved the/one share/s you will be asked if you want to check their validity.

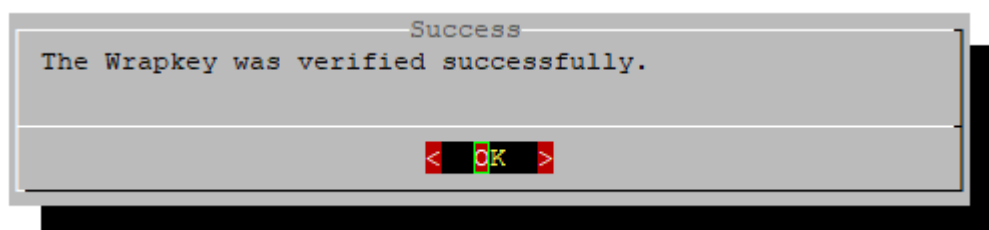


Select "Yes" to validate the shares. Select "No" to skip this step (not recommended).

Now you have to enter the threshold "2" for example. Then type in the shares. The order of the typed in shares does not matter. Be careful not to enter the same share multiple times and that you entered the right threshold.

```
Enter the threshold: 2
Enter share number 1: 2-1-8bD1fcNDBSSr602bYnzTze0LDE3eaCB4ebJoLA1b8eTFQrkp5LoMABEI63H16V2jtM0z2w
```

If you did everything correctly, this message should appear.



Now the wrapkey is stored.

Use the plain text wrapkey directly

If you selected 1 share and 1 threshold the wrapkey will be displayed in cleartext instead:


```
This is your Wrapkey:
d1c5b6c5d156ed57e4e5f2ccc4c064f01348c5e3fe2eaf6e1b3e37dcff9a2ae

It will be stored on the YubiHSM with ID:
0x0002

Save both the Wrapkey and the ID in a save location like a password manager.

Did you save the Wrapkey? [y/n]
```

This way you get a randomly generated Wrapping Key like the one you see above.

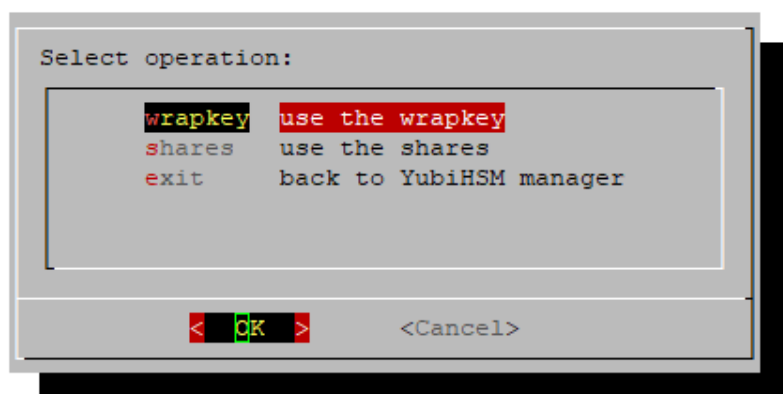
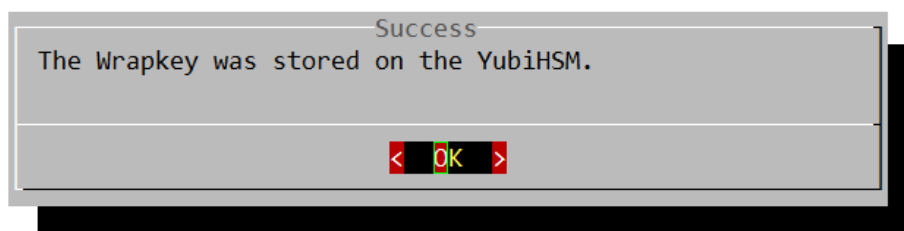
You need this information to make backups of your YubiHSM!

Note: You can use up to 16 separate applications / CA servers on one YubiHSM, with this Wrapkey you can backup all of them at once.

To confirm that you have the correct Wrapkey you have to enter it in the next screen.

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

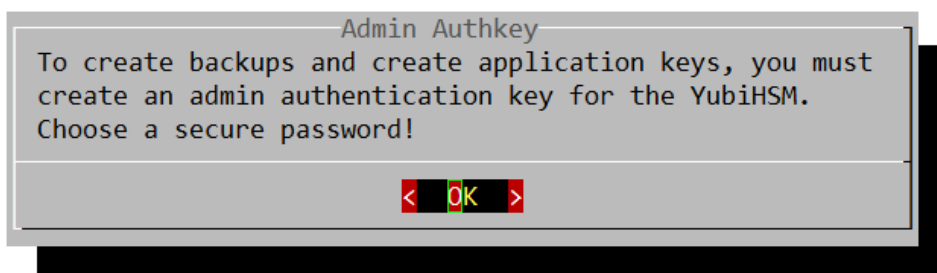
After successfully confirming the Wrapkey it is stored on the YubiHSM and you get the following message:



This selection pops up everytime when the wrapkey is needed. You can enter the wrapkey or the shares depending on your setup.

6.4.2 Creating the Admin Authentication Key

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



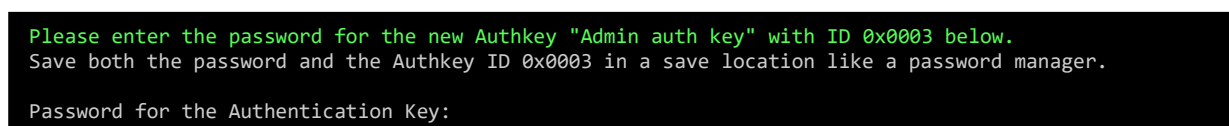
An Authkey or Authentication Key is one of the most fundamental Objects. Authentication Keys can be used to establish sessions with a YubiHSM device.

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

More information about the different Objects can be found here:

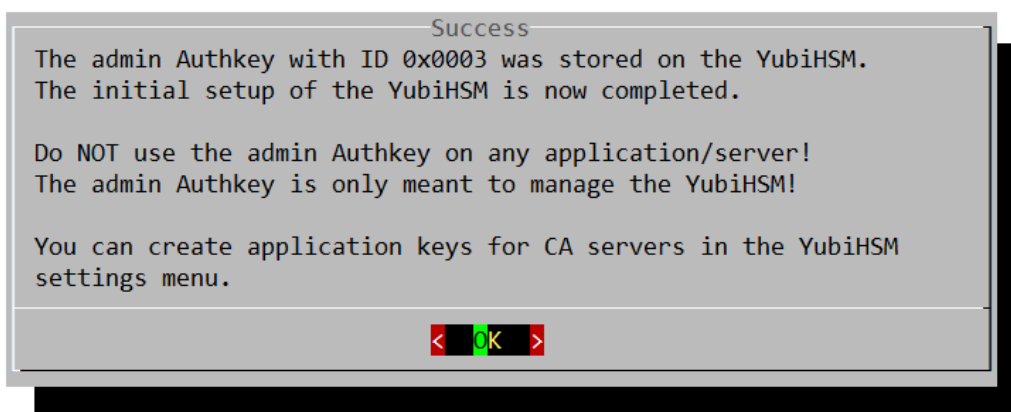
<https://developers.yubico.com/YubiHSM2/Concepts/Object.html>

After clicking "OK" you will see this message:



You should choose a very strong (randomly generated) password as this is the Admin Authkey and has unrestricted rights on the YubiHSM.

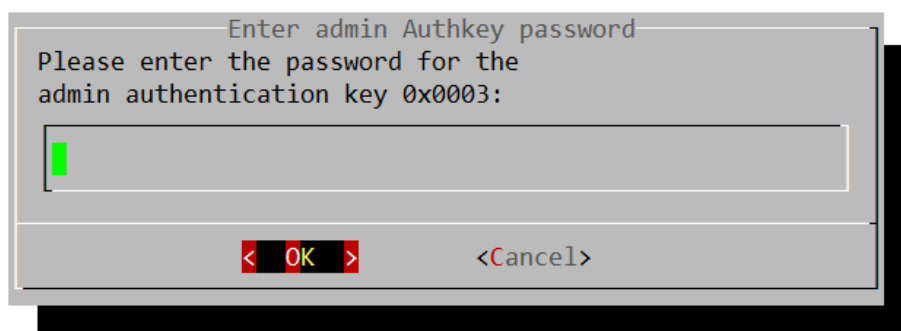
After you confirmed the password, you should see this screen:



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

6.5 Authentication Key

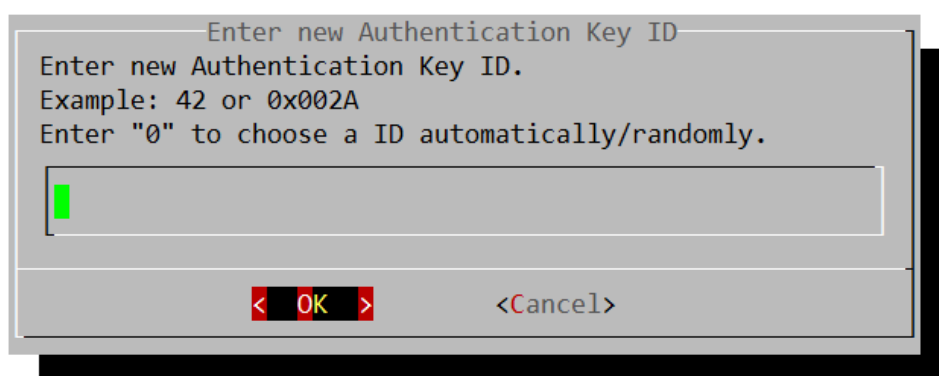
You can handle the Authkeys like user accounts (on the YubiHSM) for your applications / CA servers.



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 applications.

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

6.5.1 Authentication Key ID



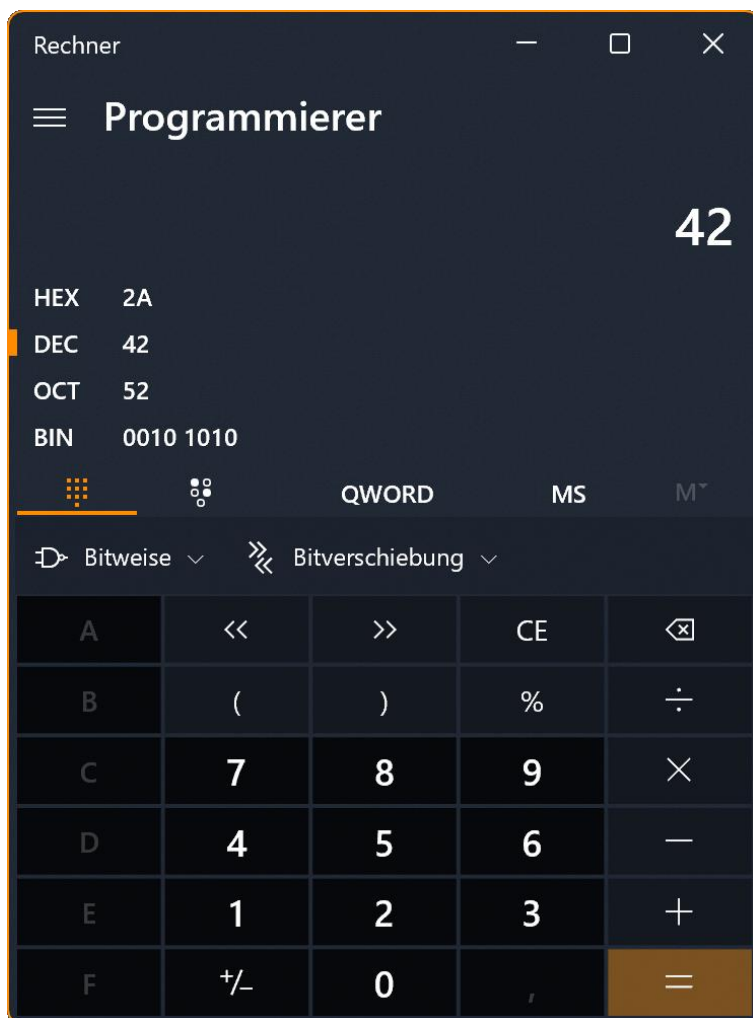
Now you can select an ID for your new Authkey. The ID is like a user name.

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, you can easily convert between decimal and hexadecimal values.

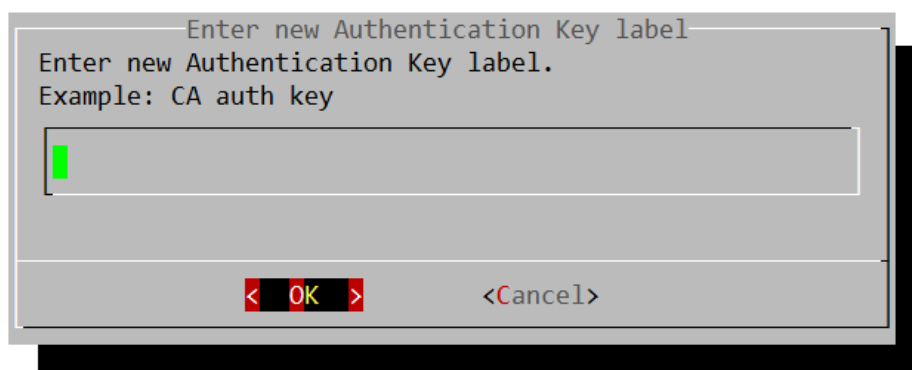
Select "HEX" and input a Hexadecimal number or "DEC" for Decimal.



More Information: <https://en.wikipedia.org/wiki/Hexadecimal>

After you entered an ID hit "OK".

6.5.2 Authentication Key label

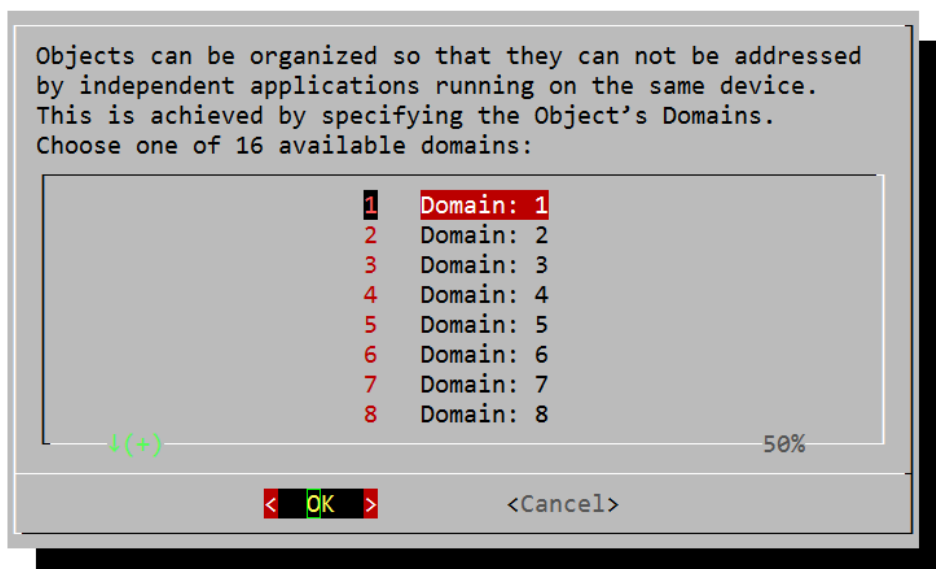


Now you can enter a label (name) for the Authentication Key to easier identify it later.

This can be anything, but we suggest to use the name of the CA 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.

6.5.3 Authentication Key Domain



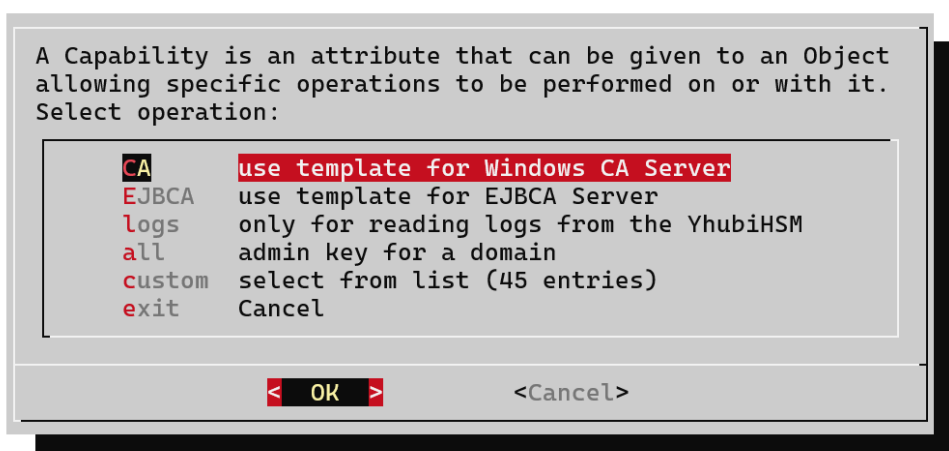
You should select a different domain for each application / CA server, otherwise they will have access to the keys from each other.

Choose "1" for the first CA server, "2" for the second CA server and so on.

More information about domains can be found here:

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

6.5.4 Authentication Key Capabilities



To select the capabilities for the new authentication key, you can use a template or select individual capabilities from a list.

6.5.5 Choose a password

Next you can enter the password for the Authentication Key.

```
Please enter the password for the new Authentication Key "example" with ID 0x002A below.
Save both the password and the Authentication Key ID 0x002A in a save location like a password
manager.
```

```
Password for the Authentication Key:
```

This ID and password you will need later on the CA server to access the YubiHSM.

After entering the password, you will see the progress of creating the Authentication Key on the YubiHSM like in the picture below.

6.5.6 Authentication Key stored on the YubiHSM

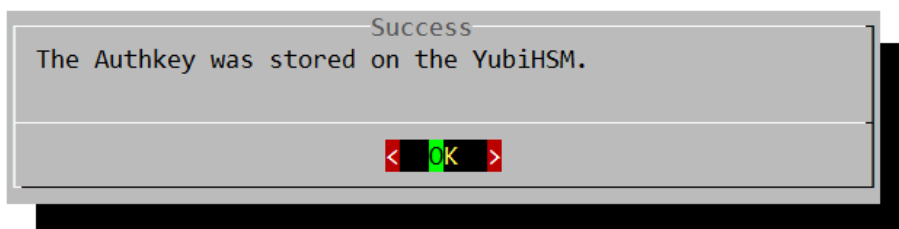
```
Using default connector URL: http://127.0.0.1:12345
Session keepalive set up to run every 15 seconds
Created session 0
Stored Authentication key 0x002a
OK ID: ^^^^^^

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.



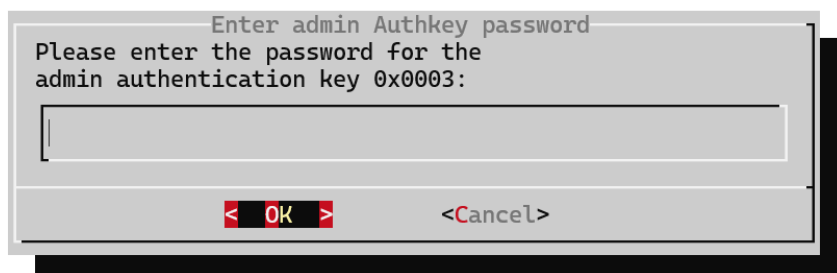
Please read [YubiHSM setup on a CA Server](#) for detailed information about setting up the YubiHSM CNG Key Storage Provider on Windows.

6.6 import

This function is used to import a private key via a .pfx file. The entire process of extracting from the CA Server and importing to the HSA can be found under [YubiHSM setup on a CA Server](#).

6.7 create

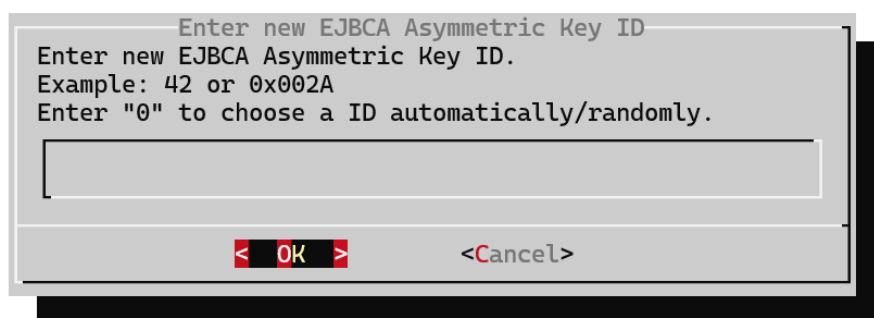
This function creates an asymmetric key for use with Linux CA.



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 applications.

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

6.7.1 Asymmetric Key ID

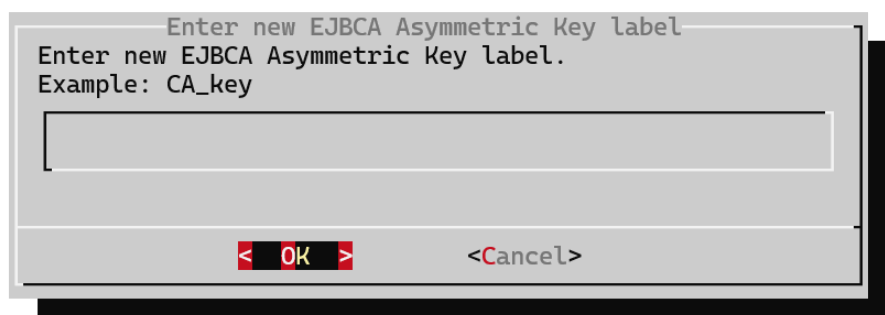


Now you can select an ID for your new Asymmetric Key. The ID is like a user name.

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).

6.7.2 Asymmetric Key label

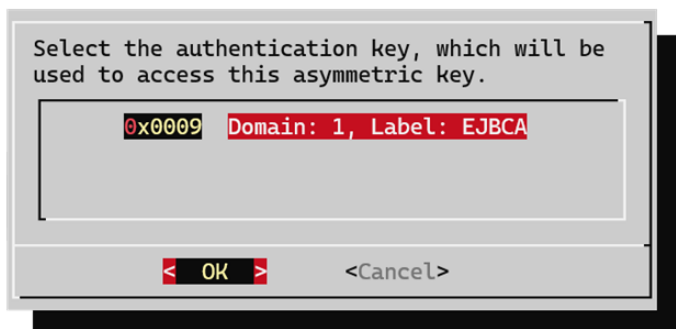


Now you can enter a label (name) for the Asymmetric Key to easier identify it later.

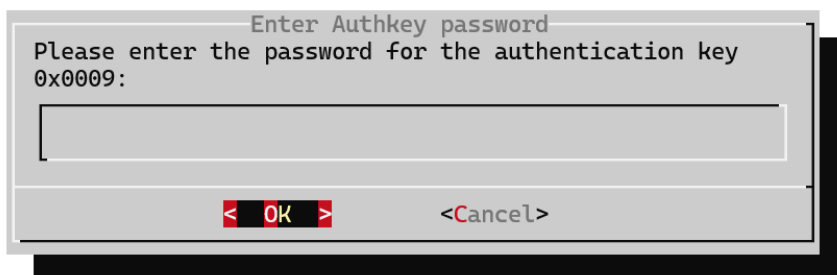
This can be anything, but we suggest to use the name of the CA server.

In the next step you can choose an Authentication Key for the Asymmetric Key.

6.7.3 Authentication Key for Asymmetric Key



After that you will be prompted to enter the password of that Authentication Key. After clicking <OK> the Asymmetric key will be generated. This will take some time.



6.7.4 Asymmetric Key stored on the YubiHSM

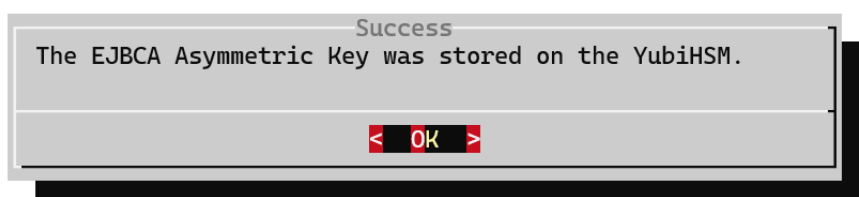
```
Using default connector URL: http://localhost:12345
Session keepalive set up to run every 15 seconds
Created session 1
Generated Asymmetric key 0x000a
OK ID: ^^^^^^

You will need the ID shown above to access this EJBCA Asymmetric 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.



6.8 backup

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

To make a backup, follow the on-screen 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.

6.9 tools

Opens a submenu with the following entries:

6.9.1 deviceinfo

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

6.9.2 objectInfo

View information about a certain object. Id, Type, Algorithm, ...

6.9.3 removeKey

If you have a key that is no longer in use or you have accidentally created a key incorrectly, you can delete it with this function.

6.9.4 listObjects

Displays all objects stored on the main YubiHSM.

6.9.5 listBackup

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.

6.9.6 domainOverview

Gives an overview of all domains and the keys stored there.

6.9.7 shell

Provides two options: to either start a shell to the internal YubiHSM or to an externally connected one by entering its serial number.

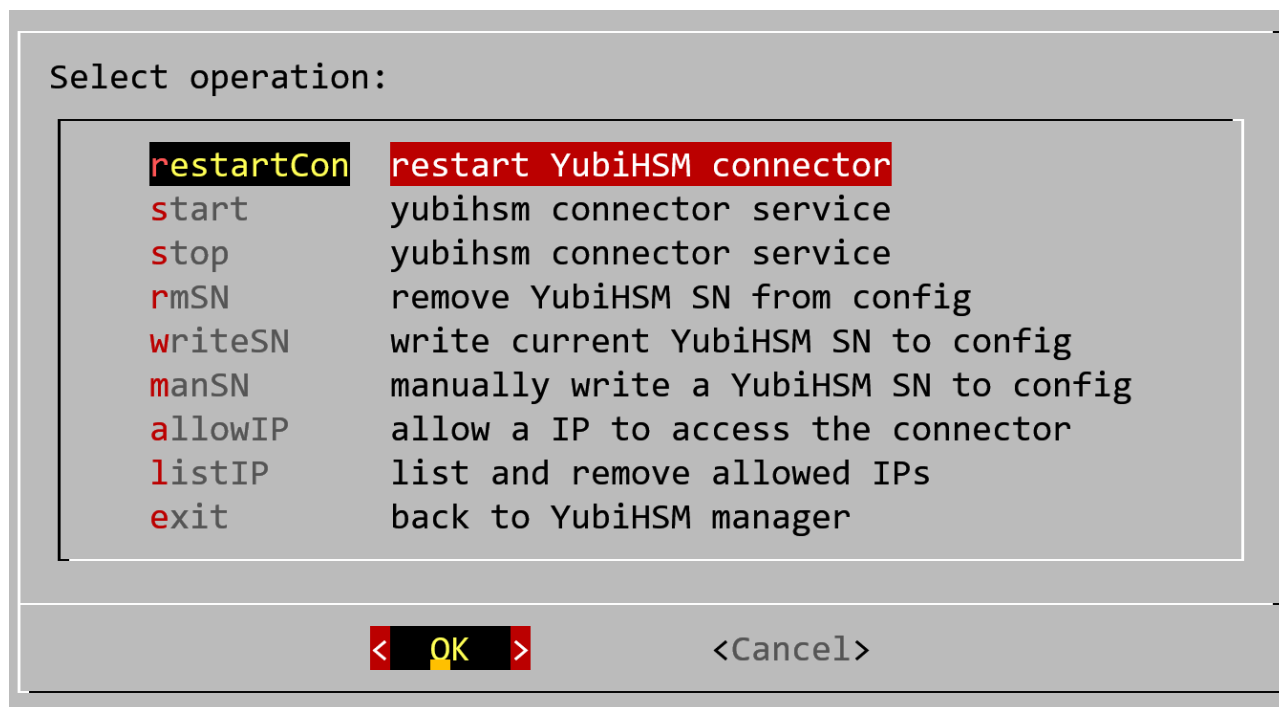
More details about the shell can be found here:

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.

6.10 connector

Opens a submenu:



6.10.1 restartCon

Restarts the YubiHSM connector on the HSA.

More information about the YubiHSM connector:

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

6.10.2 start

Starts the YubiHSM connector service.

6.10.3 stop

Stops the YubiHSM connector service.

6.10.4 rmSN

Deletes the YubiHSM serial number from the connector config.

6.10.5 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.

6.10.6 manSN

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

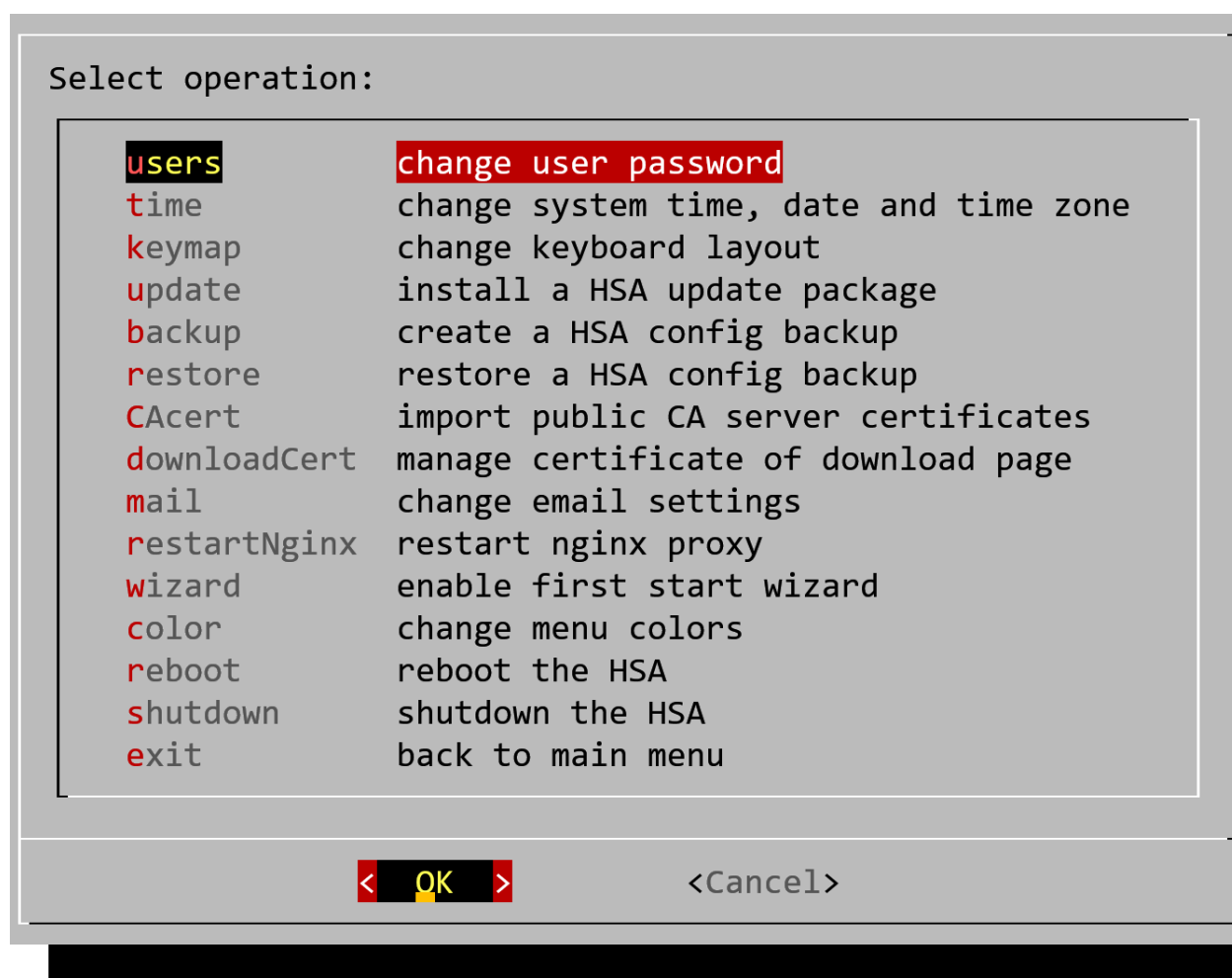
6.10.7 allowIP

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

6.10.8 listIP

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

7 HSA menu

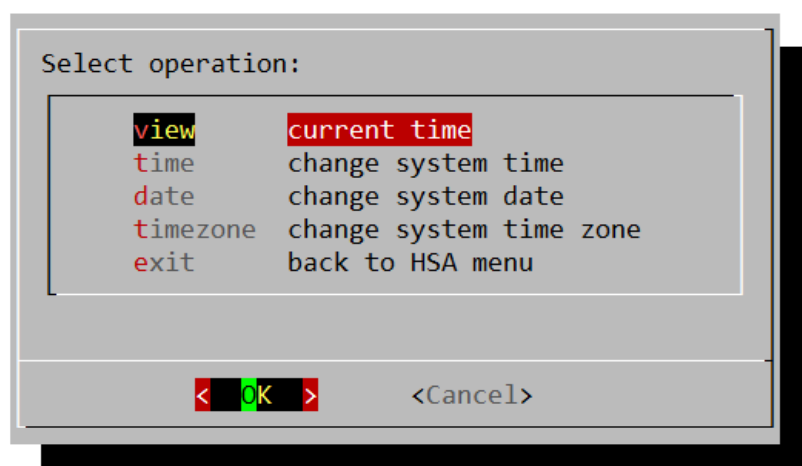


7.1 users

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

7.2 Time

Opens a submenu:

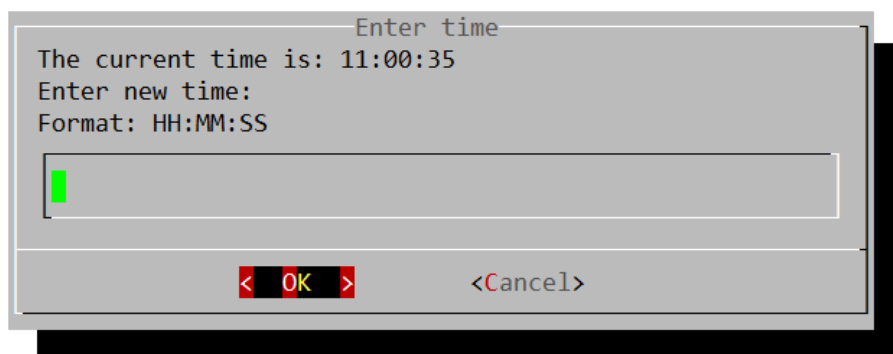


These settings are the same you can make with the [Setup Wizard](#): [Enter time](#), [Enter date](#), [Setting timezone](#).

7.2.1 View

Shows the current time on the system.

7.2.2 Time



Enter time

The current time is: 11:00:35

Enter new time:

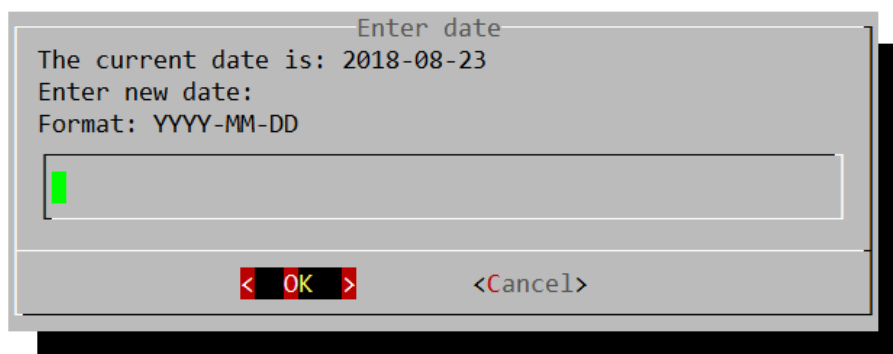
Format: HH:MM:SS

< OK > <Cancel>

Enter the current time or select “Cancel” if it 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”.

7.2.3 Date



Enter date

The current date is: 2018-08-23

Enter new date:

Format: YYYY-MM-DD

< OK > <Cancel>

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

7.2.4 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 selection which is appearing after selecting a continent.

```
The following information has been given:

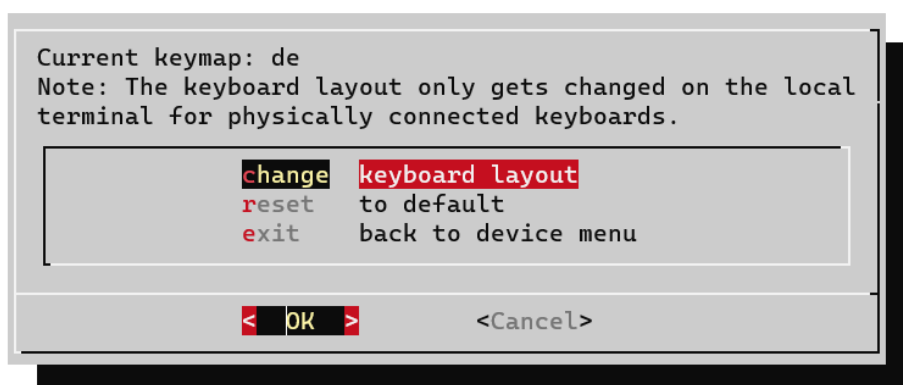
Austria

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.

7.3 keymap

Here you can change the keyboard layout on the local terminal for directly connected keyboards.



Note: Use keymaps with letters of the Latin alphabet, because letters like ω (a Greek letter) will not decode and you will see ♦ instead.

7.4 update

Updates can be installed via network or USB drive.

Please follow the on-screen instructions to install offline updates for the HSA.

The updates can be downloaded with the following link:

<https://asf.anlx.cloud/index.php/s/NNHq6S4XzGcb46r?path=%2FHARDWARE%20SECURITY%20APPLIANCE>

7.5 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 as well as certificates and keys stored on the yubiHSM!

See [The yubiHSM menu](#) > [backup](#) to create a backup from the YubiHSM.

7.6 restore

Please follow the on-screen instructions to restore backups to the HSA.

7.7 CAcert

Opens a submenu, where you can manage trusted CA certificates.

This is important for some services to be able to establish connections to servers in your network.

7.8 downloadCert

Note: The encoding of files created from this menu is PEM. Files uploaded via this menu must also be encoded in PEM.

Allows you to change the HSA web management certificate.

Create

Create a new self-signed certificate.

Import

Import an externally created certificate and private key.

Download

Download the current public certificate.

CSR

Create a certificate signing request to be signed by a CA.

CRT

Import the signed certificate which was created with a CSR.

7.9 mail

Enter the mail submenu.

Server

Set the server address and port.

Authentication

Disable or enable SMTP authentication and enter user and password.

TLS

Enable or disable TLS.

Sender

Set the sender mail address for sending mails.

Receivers

Add a list of receiver addresses that will always be notified.

Single services may add their own addresses which also receive the mail, this can be configured for the services itself.

7.10 restartNginx

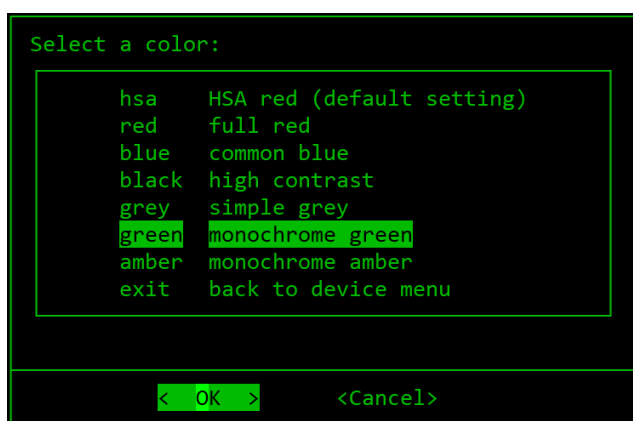
Restarts the nginx reverse proxy.

7.11 wizard

This enables or disables the [Setup Wizard](#).

7.12 color

Provides options for customizing menu colors.



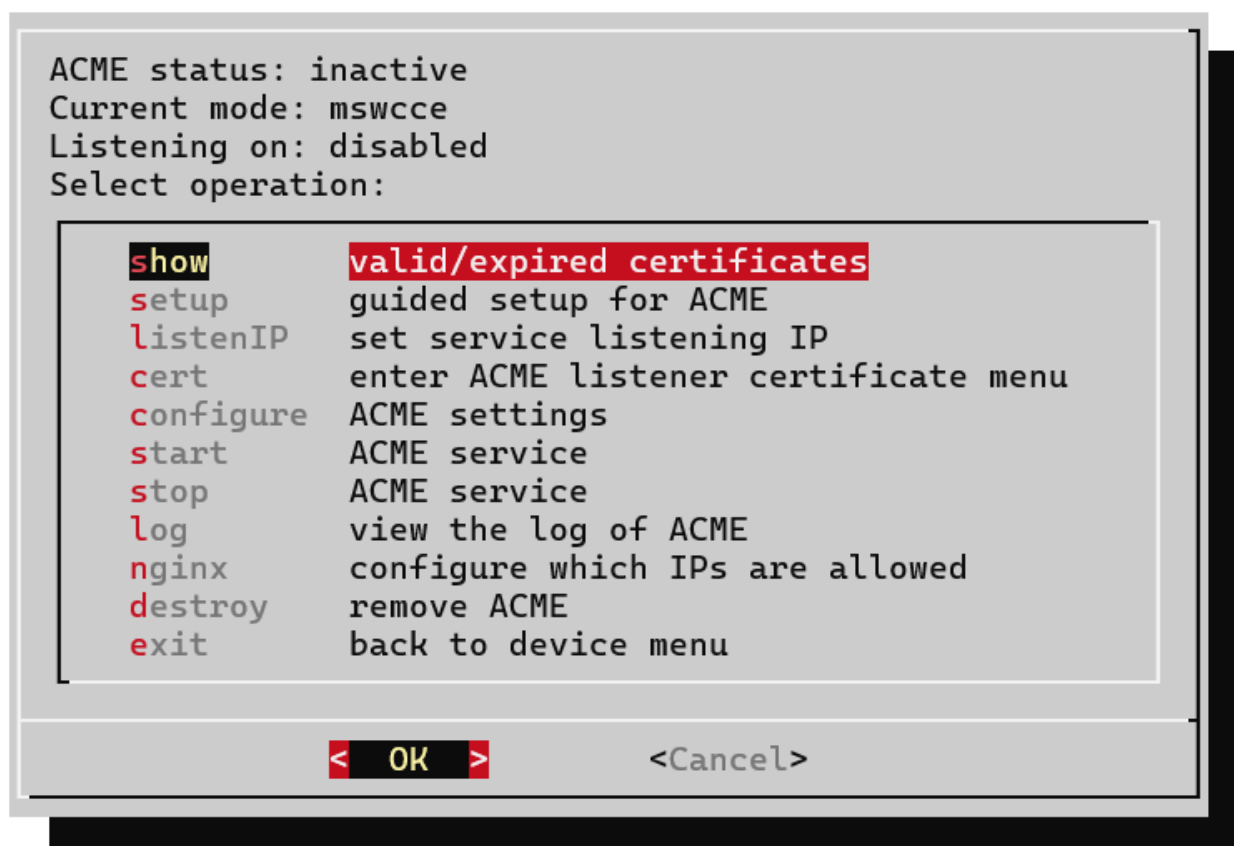
7.13 reboot

Reboots the HSA.

7.14 shutdown

Shutdown the HSA.

8 ACME menu



8.1 show

Opens a submenu to display the following information:

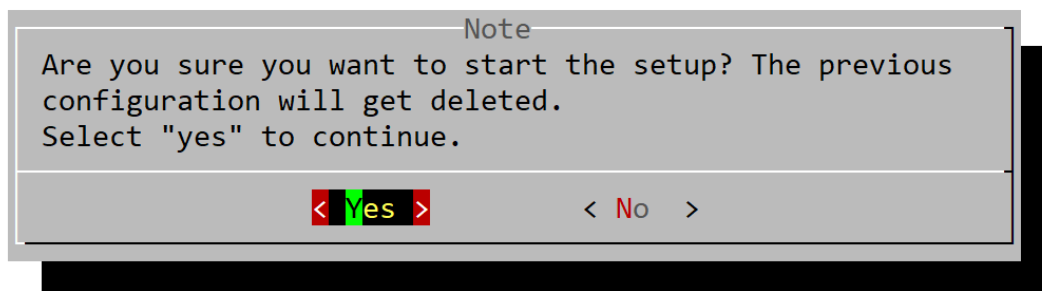
- Latest 20 valid certificates.
- Latest 20 expired certificates.
- Certificates expiring in the next 14 days.

8.2 setup

Starts the guided setup for ACME on the HSA.

Before you start setting up ACME, you will need to configure your CA if you have not done that so far. See [Set up the CA for ACME](#) if you only use ACME. When you also use a YubiHSM module, go to [YubiHSM setup on a CA Server](#).

If you are going to use the Let's Encrypt Mode, look at the following [requirements](#).



Select “yes” to start the setup of ACME on your HSA. Make sure you have your CA configured.

You will be asked for the following information:

- Select the Mode
- mswcce
 - IP of CA server
 - User account, which should be used to access the server.
 - Password for that account.
 - IP of a dns server.
 - Upload of the CA bundle to authenticate the CA server.
 - What template should be used for signing the certificates.
 - The basic ACME setup is now complete.
- acme-ca
 - Let’s Encrypt instance
 - E-mail for Let’s Encrypt

Reminder:

For ACME to work, you must make DNS entries for the clients to verify that they are allowed to get a certificate.

8.3 listenIP



Please ensure that a different IP is used for each of the YubiHSM, ACME and EST service.

Here you can select an IP on which the service should listen for incoming connections. Additional IPs can be added via network settings for an interface or if you have a cluster, in the cluster menu.

8.4 cert

Note: The encoding of files created from this menu is PEM. Files uploaded via this menu must also be encoded in PEM.

Enter the connector certificate submenu to manage the public https certificate for the ACME service.

The following options are available:

Create

Create a new self signed certificate.

Import

Import an externally created certificate and private key.

Download

Download the current public certificate.

CSR

Create a certificate signing request to be signed by a CA.

Note: This is not recommended for the YubiHSM connector as the CA will probably need the YubiHSM to sign certificates, and this connection should work independent of it.

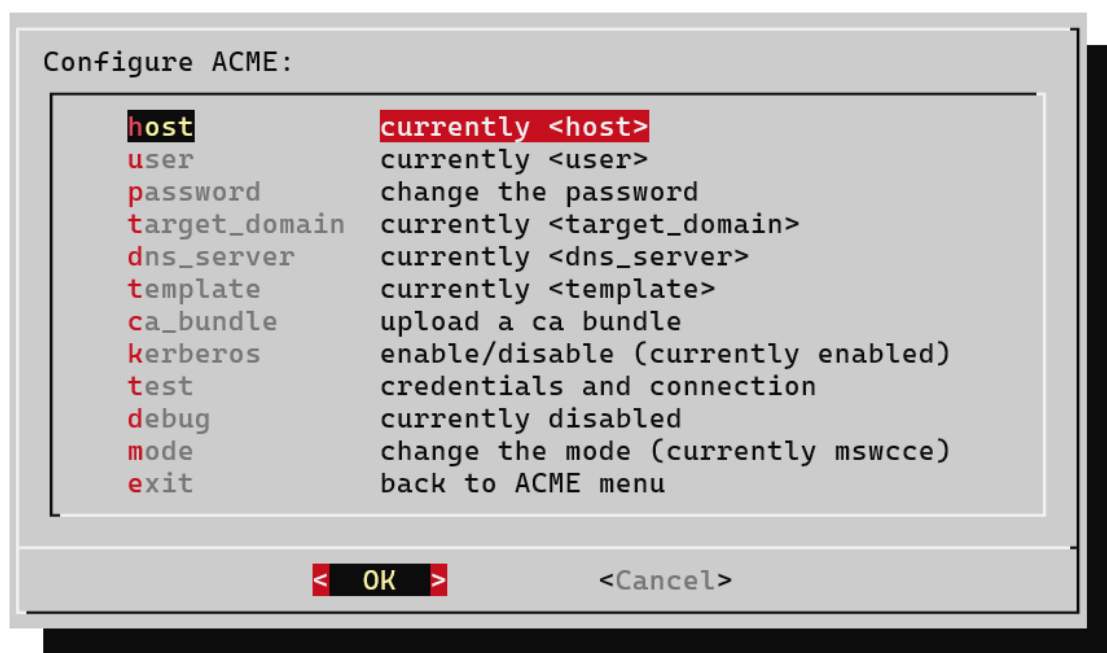
CRT

Import the signed certificate which was created with a CSR.

8.5 configure

Opens a menu where you can configure the following ACME settings.

8.5.1 Mode – mswcce



Here are all the menu options for the MSWCCE mode with a short description.

host

The menu option “host” asks for the IP or DNS name of the Windows CA that will be used.

user

The menu point “user” wants the username that will be used for authentication to the Windows CA.

password

The menu option “password” wants the password of the username you have specified.

target_domain

This menu item is optional, but it is required in order for the authentication to the Windows CA to work with Kerberos.

dns_server

Here you will be asked to enter the IP address of a DNS server.

template

This menu options wants the certificate template you created on your Windows CA. This template is then used when a certificate is enrolled over ACME.

ca_bundle

The menu option “ca_bundle” prompts you to upload the CA bundle.

kerberos

This allows you to toggle whether Kerberos should be used to authenticate to the Windows CA.

debug

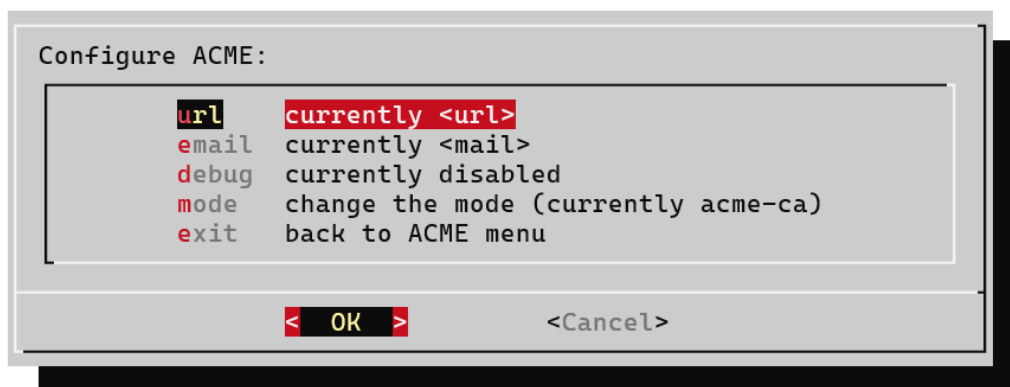
The menu options “debug” enables or disables the debug mode. A restart of the ACME container is required after enabling or disabling.

mode

Here you change the ACME mode to the following:

- mswcce: ACME server for Windows CA
- acme-ca: proxy for ACME

8.5.2 Mode – acme-ca



Here are all the menu options for the ACME-CA mode with a short description.

url

This menu option wants the URL of a Let's Encrypt instance.

email

The menu point "email" will ask you to enter the email for Let's Encrypt.

debug

The menu options "debug" enables or disables the debug mode. A restart of the ACME container is required after enabling or disabling.

mode

Here you change the ACME mode to the following:

- mswcce: ACME server for Windows CA
- acme-ca: proxy for ACME

8.6 start

Starts ACME.

8.7 stop

Stop ACME.

8.8 log

Shows the logs of ACME.

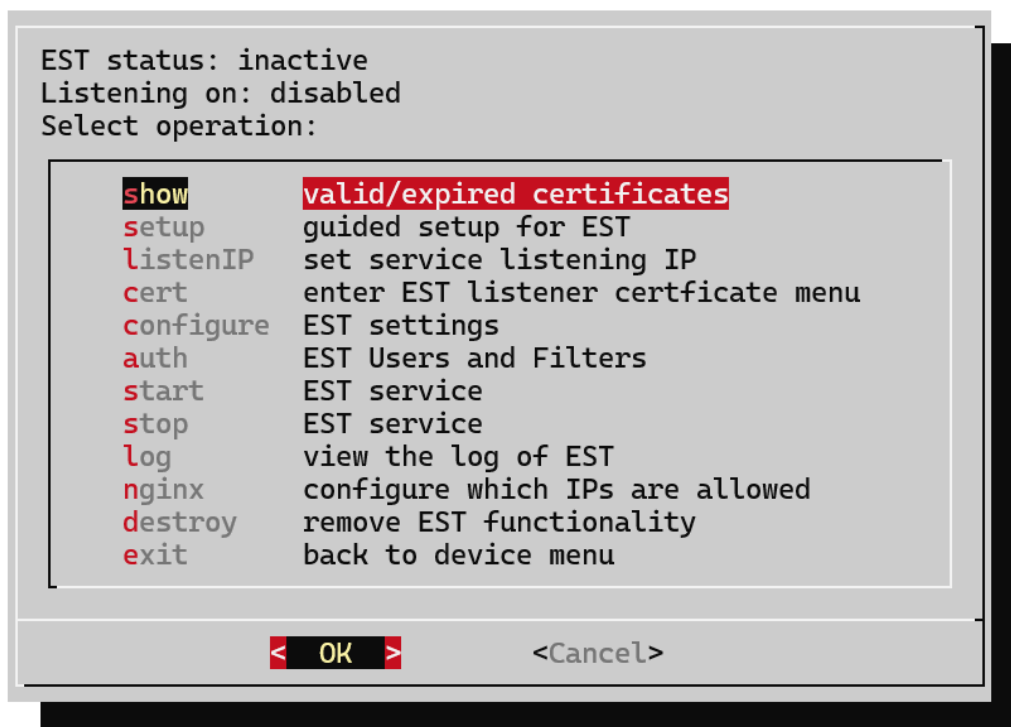
8.9 nginx.

Configure which IPs are allowed to access ACME.

8.10 destroy

Remove ACME from an HSA or from a single node if it is in a cluster. This will delete the configuration files related to ACME.

9 EST Menu

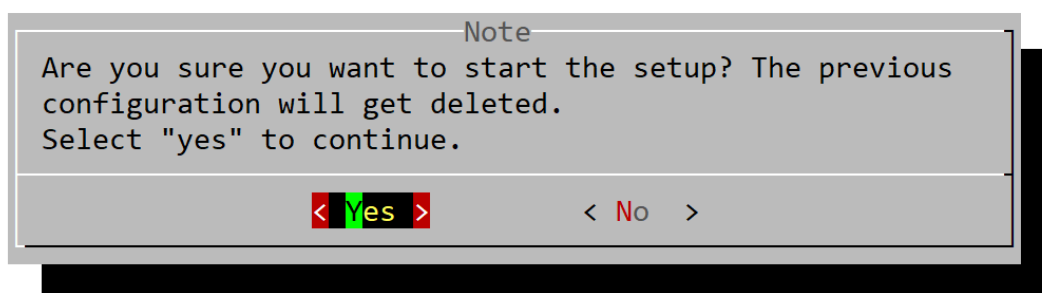


9.1 show

Opens a submenu to display the following information:

- valid certificates.
- expired certificates.
- Certificates expiring in the next 14 days.

9.2 setup



Select "yes" to start the setup of EST on your HSA. Make sure you have your CA configured.

You will be prompted for the following information

- FQDN of the CA server
- User account to be used to access the server.

- Password for this account.
- IP of a DNS server.
- The target domain. E.g. est.lab
- If Kerberos is to be used.
- Upload the CA bundle to authenticate the CA server.
- The basic EST setup is now complete.

9.3 listenIP



Please ensure that a different IP is used for each of the YubiHSM, ACME and EST service.

Here you can select an IP on which the service should listen for incoming connections. Additional IPs can be added via network settings for an interface or if you have a cluster, in the cluster menu.

9.4 cert

Note: The encoding of files created from this menu is PEM. Files uploaded via this menu must also be encoded in PEM.

Enter the connector certificate submenu to manage the public https certificate for the EST service.

The following options are available:

Import

Import an externally created certificate and private key.

CSR

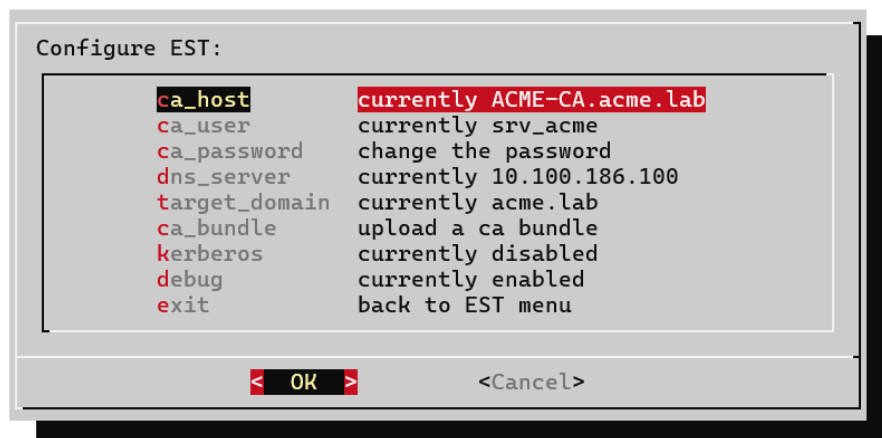
Create a certificate signing request to be signed by a CA.

Note: This is not recommended for the YubiHSM connector as the CA will probably need the YubiHSM to sign certificates, and this connection should work independent of it.

CRT

Import the signed certificate which was created with a CSR.

9.5 configure



Here are all the menu options for configuring EST with a short description.

ca_host

The menu option “ca_host” asks for the IP or DNS name of the Windows CA that will be used.

ca_user

The menu point “ca_user” wants the username that will be used for authentication to the Windows CA.

ca_password

The menu option “ca_password” wants the password of the username you have specified.

dns_server

Here you will be asked to enter the IP address of a DNS server.

target_domain

This menu option wants you to enter the target domain.

ca_bundle

The menu option “ca_bundle” prompts you to upload the CA bundle.

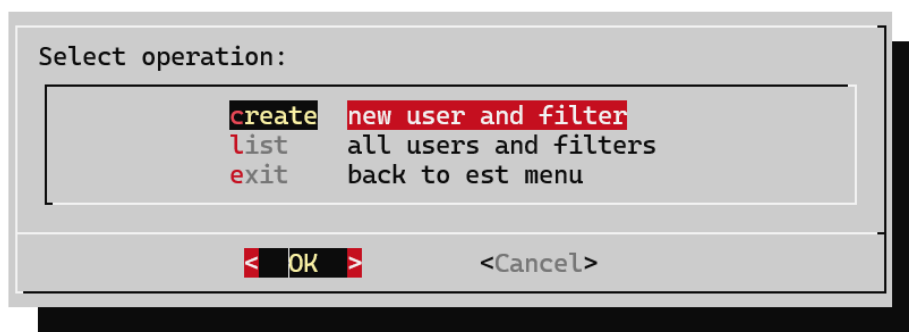
kerberos

This allows you to toggle whether Kerberos should be used to authenticate to the Windows CA.

debug

The menu options “debug” enables or disables the debug mode. A restart of the EST container is required after enabling or disabling.

9.6 auth



In the auth menu you can manage users for authentication to EST.

create

Create a new user with regex filters.

list

List all existing users for viewing, editing or deleting.

9.7 start

Start EST.

9.8 stop

Stop EST.

9.9 log

Show the log of EST

9.10 nginx

Configure which IPs are allowed for EST.

9.11 destroy

Remove EST from an HSA or from a single node if it is in a cluster. This will delete the configuration files related to EST.

10 Cluster menu



10.1 clusterWizard

Starts the wizard to set up a new cluster node. The cluster contains two functionalities: Failover and virtual IP.

10.2 show

Show where cluster IPs are running and their usage (Default, YubiHSM, ...).

10.3 addIP

Add an IP address to the cluster.

All configured IPs work in failover mode, and always run on the same node together. In case the first node fails, the second node takes over.

10.4 deleteIP

Provides a list of IPs which can be selected to delete them.

10.5 createClusterSeed

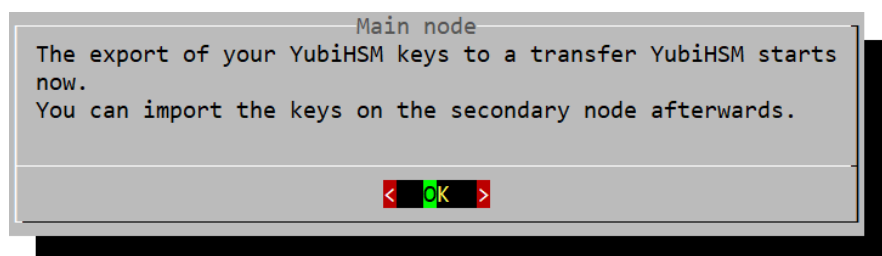
Creates the seed file based on the configuration of this node. By importing this file to other nodes, you can add them to the cluster.



The cluster seed should be created when the configuration of the first node is complete.

The following configurations will be copied:

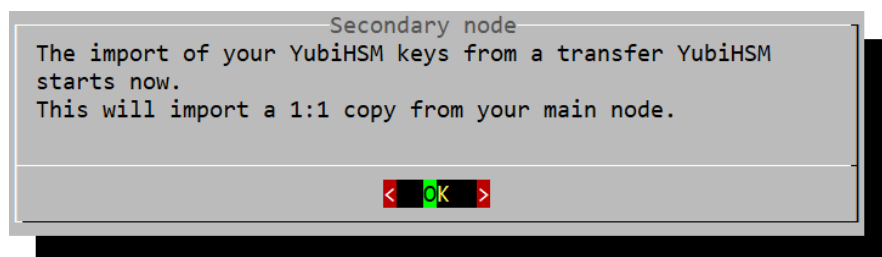
- General config (NTP, ...)
- listen IPs of YubiHSM/ACME/EST
- YubiHSM config
- ACME config
- EST config



With the seed file the HSA configuration gets exported but not the objects/keys on the YubiHSM. For this a separate transfer YubiHSM is required to create a 1:1 copy on the target node.

10.6 importClusterSeed

Imports a seed file to join a node to a cluster and imports YubiHSM objects from a transfer YubiHSM.



10.7 disable

All cluster functions are stopped and can be restarted with the menu item "enable".

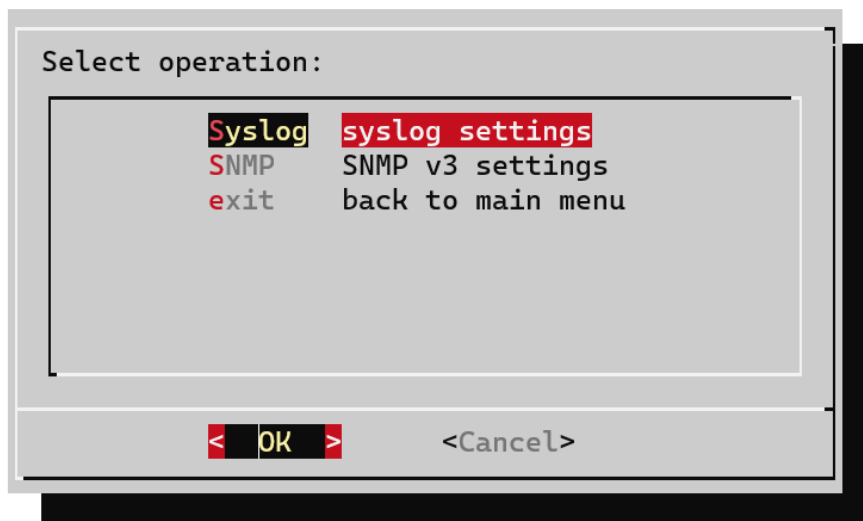
10.8 enable

Starts the cluster services after they were stopped with the menu item "disable".

10.9 destroy

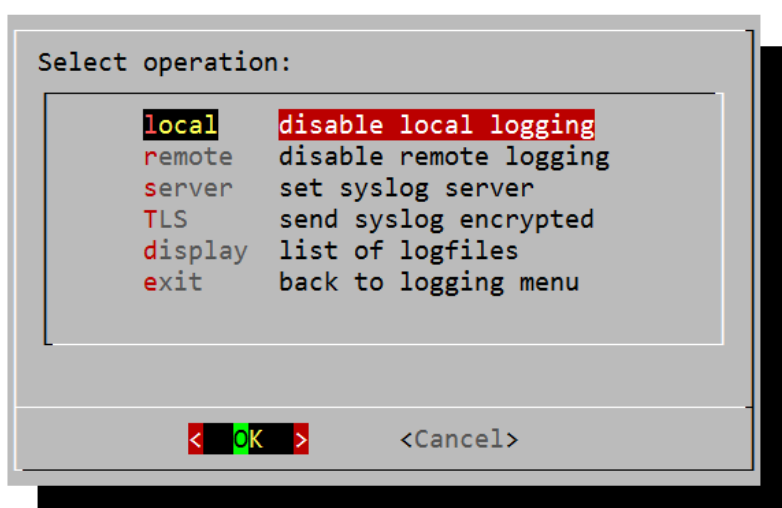
Removes all cluster functions from a node.

11 Logging menu



11.1 Syslog

Opens a submenu:



11.1.1 local

Toggles between enabled or disabled local logging.

11.1.2 remote

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

11.1.3 server

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

11.1.4 TLS

Opens a submenu where you can configure syslog TLS settings.

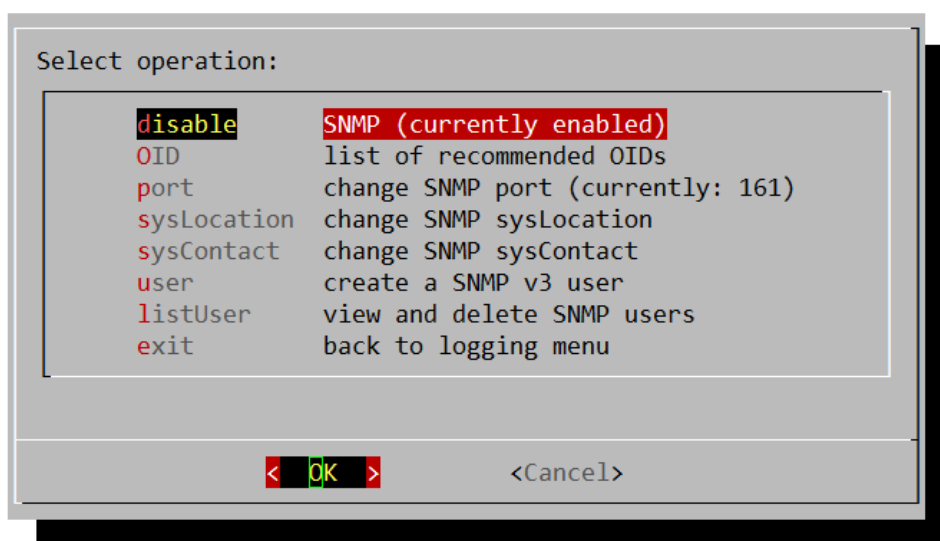
- “enable”/“disable” TLS (toggles between enabled or disabled).
- “certCA” upload server CA certificate
- “certClient” upload client certificate
- “certKey” upload client certificate key
- “enaClCr”/“disClCr” enable/disable client cert
- With “AuthMode” you can choose between the following authentication methods:
 - anon - anonymous authentication
 - x509/fingerprint - certificate fingerprint authentication
 - x509/certvalid - certificate validation only
 - x509/name - certificate and subject name validation

11.1.5 display

Displays a list of all log files from which you can select one to read.

11.2 SNMP

Opens a submenu to configure SNMP v3.



11.2.1 enable/disable

Toggle switch.

11.2.2 OID

Displays a list of useful 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
```

11.2.3 port

Changes the SNMP port.

11.2.4 sysLocation

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

11.2.5 sysContact

Can change the primary contact for the device.

11.2.6 user

Can create 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).

11.2.7 listUser

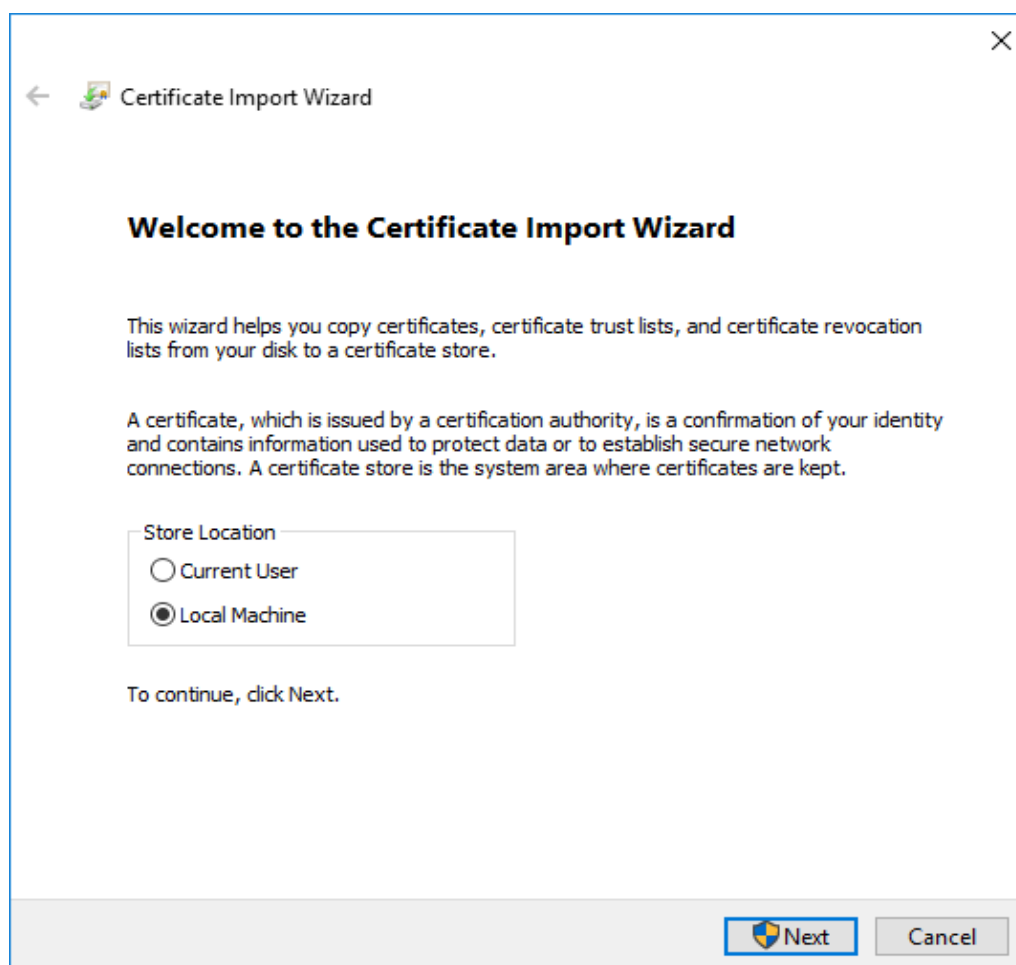
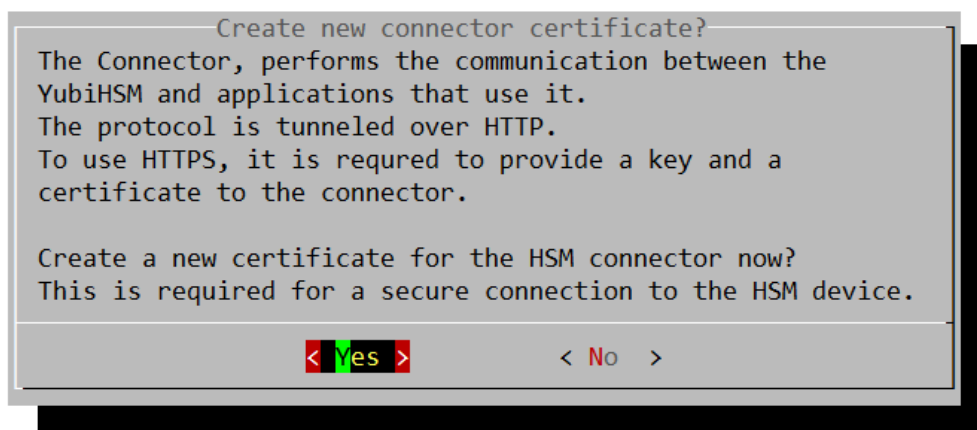
Lists all SNMP v3 users, select one and click "OK" to delete it or select "Exit" to go back.

12 YubiHSM setup on a Windows CA

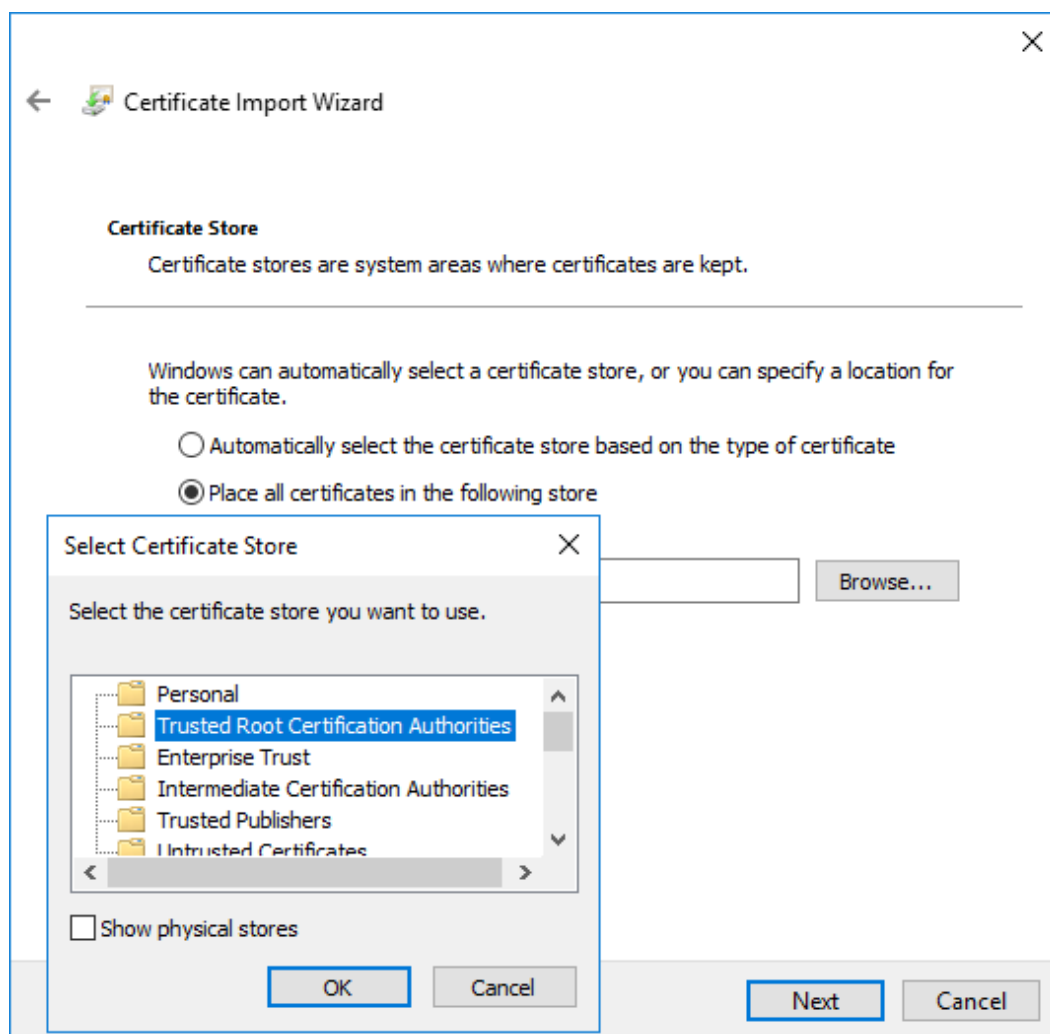
12.1 Installing the connector certificate

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

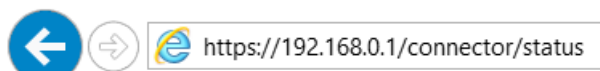
This certificate was created and downloaded on the HSA Box. If this point was skipped in the wizard, it must be done now. On your HSA, navigate to YubiHSM -> Connector -> cert -> create. Detailed instructions on the creation process can be found under [Creating a new connector certificate](#).



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



To test if the certificate and the connection to the HSA works correctly, please open Internet Explorer on the CA server and enter:
<https://192.168.0.1/connector/status> (Replace the IP with the one currently set on the HSA.)



```
status=OK
serial=000[REDACTED]
version=2.0.0
pid=432
address=localhost
port=12345
```

If everything works correctly, you should be able to access this page without any certificate warnings.

It is recommended to allow access to the YubiHSM only from the IPs of the used applications. You can do this in: The yubiHSM menu > connector > allowIP

12.2 Installing the YubiHSM Key Storage Provider



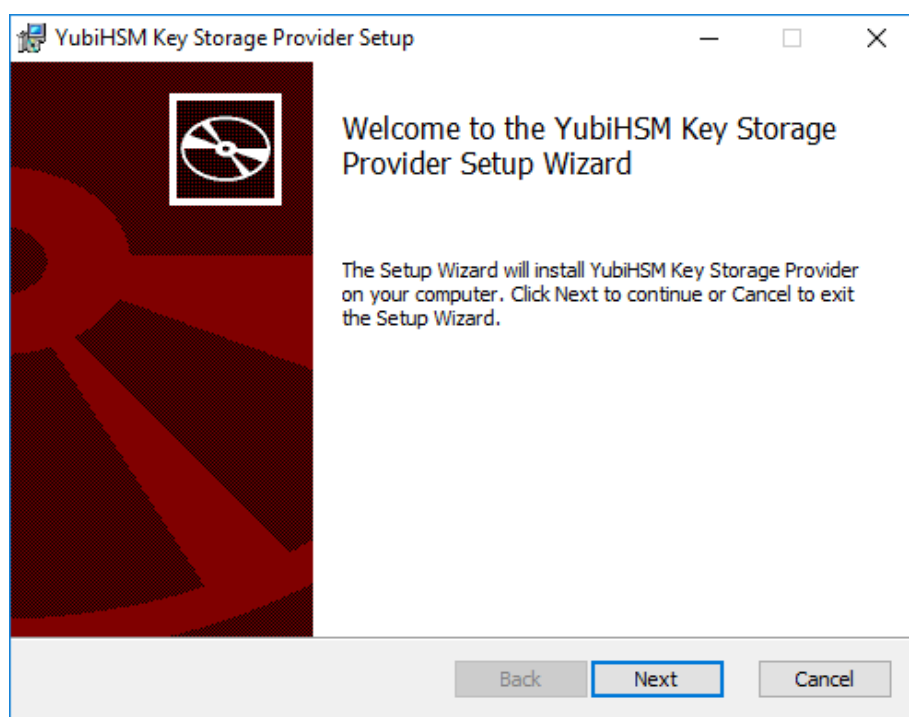
Please make sure that “Creating an application Authentication Key” is completed before proceeding, as that key is required for this step.

Download the Setup from the following Link:

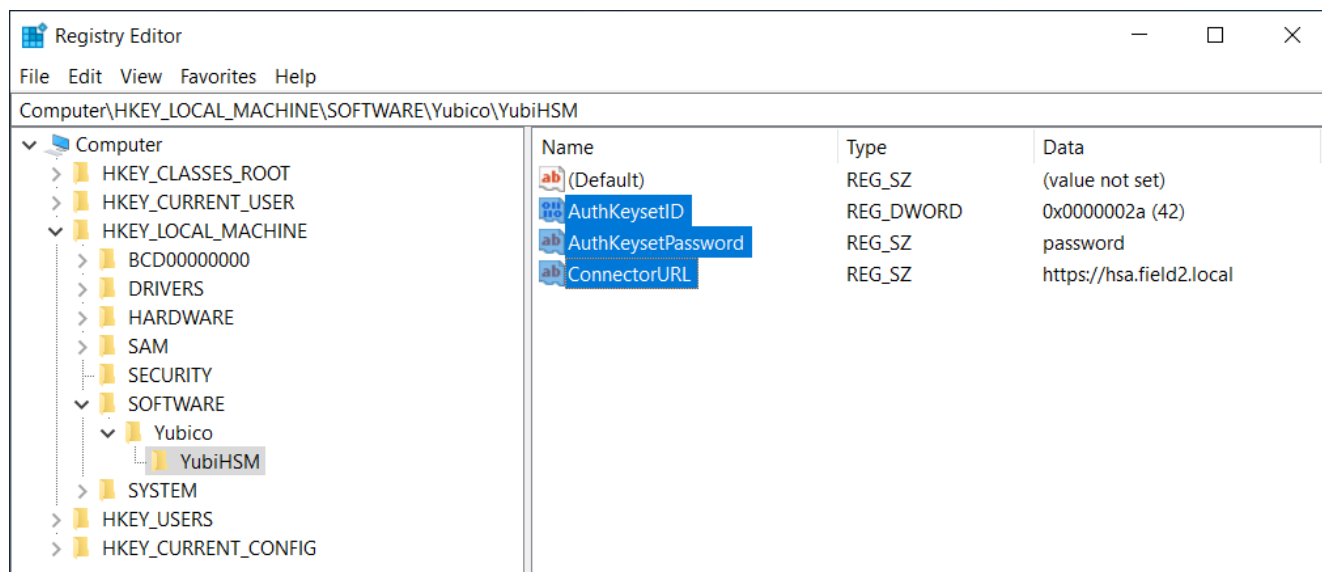
<https://developers.yubico.com/YubiHSM2/Releases/>

Select: yubihsm2-sdk-20??-??-windows-amd64.zip

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

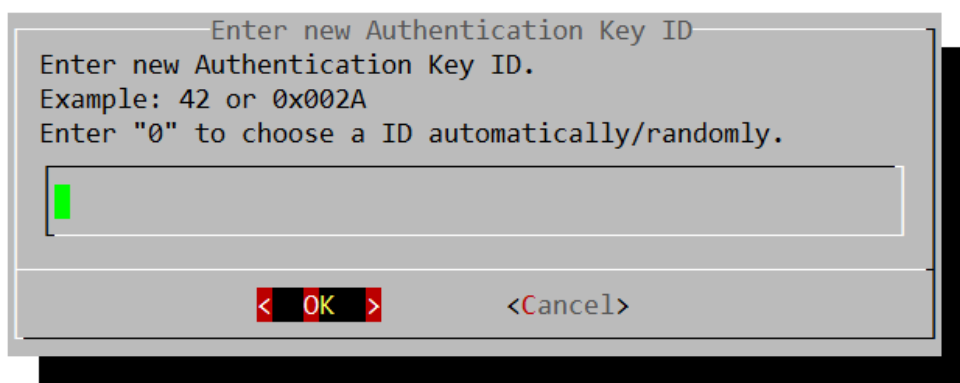


Follow the YubiHSM Key Storage Provider Setup “Wizard” until it is completed and then open the Registry Editor and navigate to “Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Yubico\YubiHSM”.



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

- “AuthKeysetID” is the ID for the 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:

```
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 Authentio Key in the future!

Did you save the ID? [y/n]
```

- “AuthKeysetPassword” is the password specified for the authentication key.
- “ConnectorURL” is https:// followed by the IP or FQDN of the HSA Box (without port).

Check the correct installation of the YubiHSM Key Storage Provider:

- Start a CMD/Powershell window as Administrator on the Windows System.
- Execute: `#> certutil -csplist`
- Must contain "Provider Name: YubiHSM Key Storage Provider".

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator.FIELD2> certutil -csplist
Provider Name: Microsoft Base Cryptographic Provider v1.0
Provider Type: 1 - PROV_RSA_FULL

Provider Name: Microsoft Base DSS and Diffie-Hellman Cryptographic Provider
Provider Type: 13 - PROV_DSS_DH

Provider Name: Microsoft Base DSS Cryptographic Provider
Provider Type: 3 - PROV_DSS

Provider Name: Microsoft Base Smart Card Crypto Provider
Provider Type: 1 - PROV_RSA_FULL

Provider Name: Microsoft DH SChannel Cryptographic Provider
Provider Type: 18 - PROV_DH_SCHANNEL

Provider Name: Microsoft Enhanced Cryptographic Provider v1.0
Provider Type: 1 - PROV_RSA_FULL

Provider Name: Microsoft Enhanced DSS and Diffie-Hellman Cryptographic Provider
Provider Type: 13 - PROV_DSS_DH

Provider Name: Microsoft Enhanced RSA and AES Cryptographic Provider
Provider Type: 24 - PROV_RSA_AES

Provider Name: Microsoft RSA SChannel Cryptographic Provider
Provider Type: 12 - PROV_RSA_SCHANNEL

Provider Name: Microsoft Strong Cryptographic Provider
Provider Type: 1 - PROV_RSA_FULL

Provider Name: Microsoft Software Key Storage Provider
Provider Name: YubiHSM Key Storage Provider
Provider Name: Microsoft Passport Key Storage Provider

Provider Name: Microsoft Platform Crypto Provider
Microsoft Platform Crypto Provider: The device that is required by this cryptographic provider
is not ready for use.

Provider Name: Microsoft Smart Card Key Storage Provider
CertUtil: -csplist command FAILED: 0x80090030 (-2146893776 NTE_DEVICE_NOT_READY)
CertUtil: The device that is required by this cryptographic provider is not ready for use.
```

The installation was successful, if "YubiHSM Key Storage Provider" is listed.

Now please select only one of the following steps to proceed:

- [New CA Server](#)
- [Migrate existing \(root\) CA certificate](#)

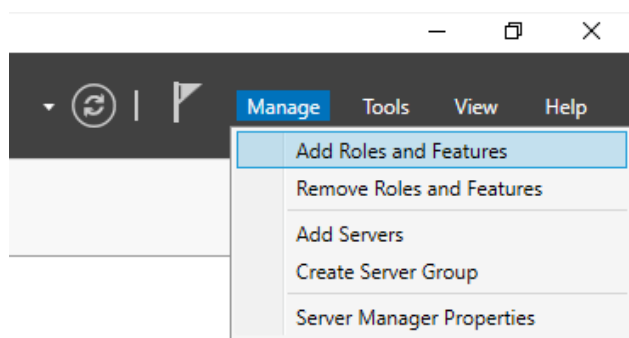
12.3 New CA Server



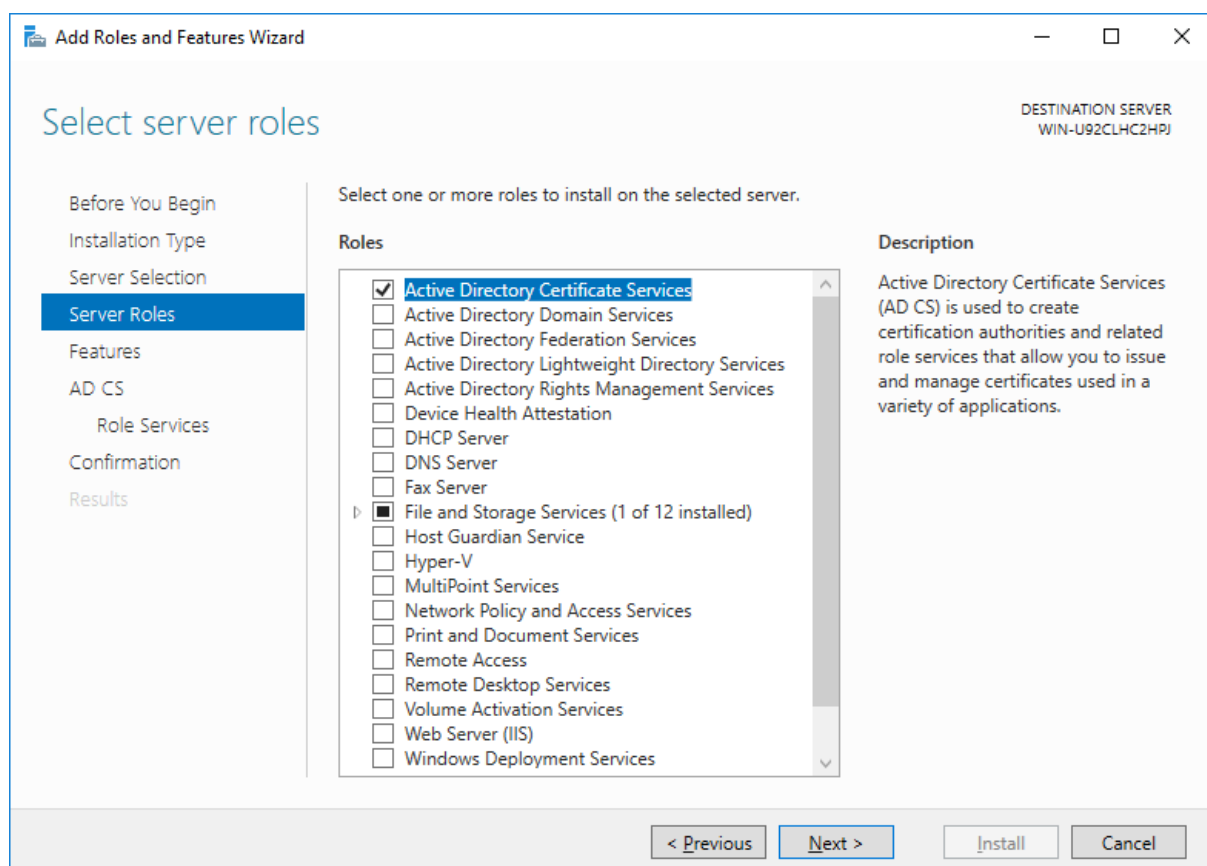
Please make sure that “Creating an application Authentication Key” is completed before proceeding. As shown in “Installing the YubiHSM Key Storage Provider”.

12.3.1 Add the CA Role

Select “Add Roles and Features” on the CA Server.

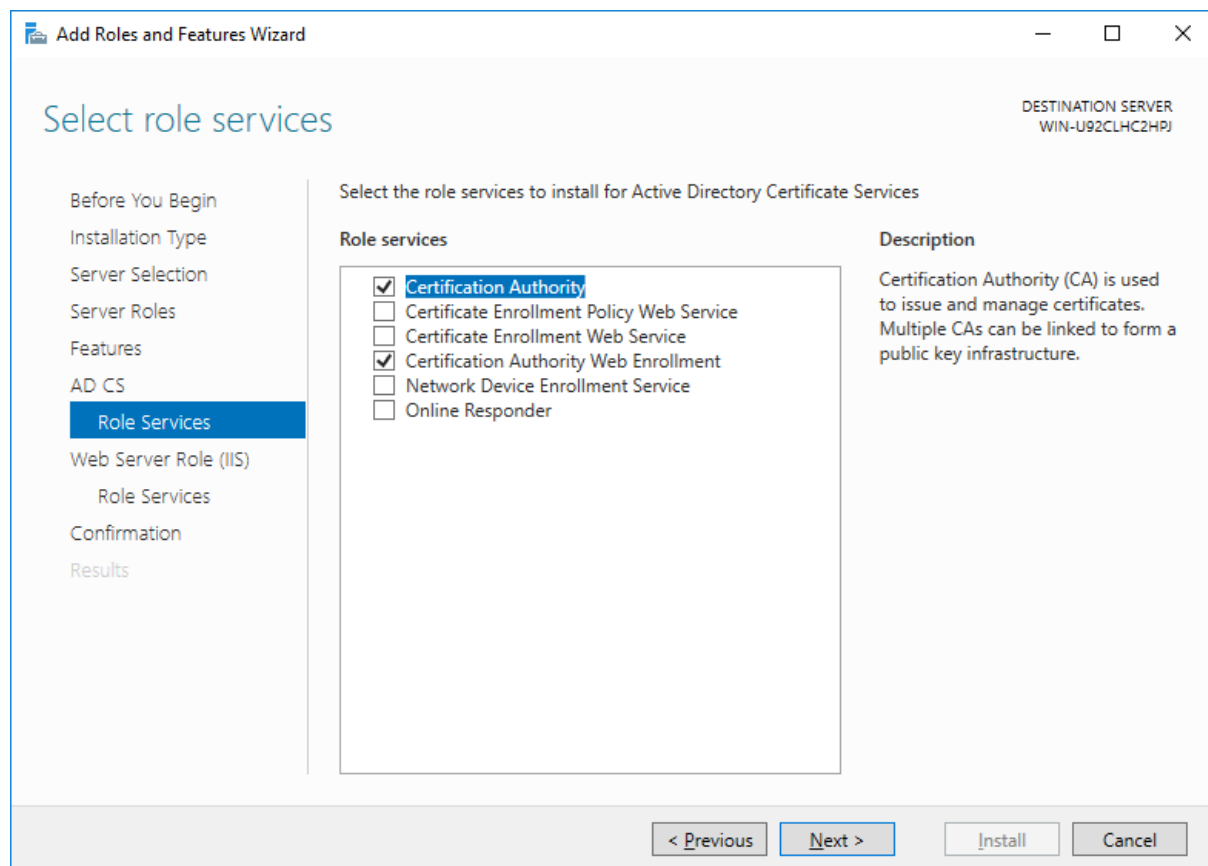


Follow the wizard until “Server Roles” and select “Active Directory Certificate Services”.



Proceed with the wizard.

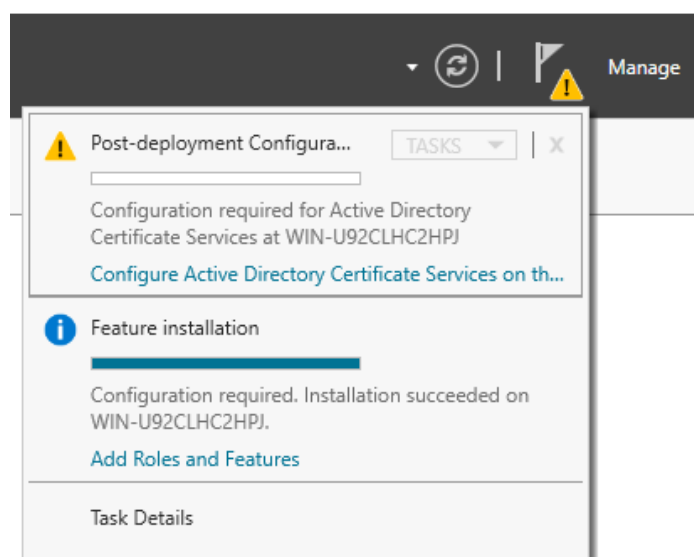
When you reach “Role Services” select “Certification Authority” and “Certification Authority Web Enrollment”.



Proceed with the wizard until it's finished.

12.3.2 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.

The screenshot shows the 'AD CS Configuration' wizard window. The title bar reads 'AD CS Configuration'. The main window has a left-hand navigation pane with the following items: 'Credentials', 'Role Services' (highlighted in blue), 'Setup Type', 'CA Type', 'Private Key', 'Cryptography', 'CA Name', 'Validity Period', 'Certificate Database', 'Confirmation', 'Progress', and 'Results'. The main area is titled 'Role Services' and contains the heading 'Select Role Services to configure'. Below this heading is a list of services with checkboxes:

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

 In the top right corner of the main area, it says 'DESTINATION SERVER WIN-U92CLHC2HPJ.test.local'. At the bottom of the main area, there is a link that says 'More about AD CS Server Roles'. At the bottom of the window, there are four buttons: '< Previous', 'Next >' (which is highlighted with a dashed border), 'Configure', and 'Cancel'.

AD CS Configuration

DESTINATION SERVER
WIN-U92CLHC2HPJ.test.local

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.

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

☐ **S**tandalone 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](#)

< 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.

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

☐ **S**ubordinate 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

AD CS Configuration

DESTINATION SERVER
WIN-U92CLHC2HPJ.test.local

Cryptography for CA

Credentials

Role Services

Setup Type

CA Type

Private Key

Cryptography

CA Name

Validity Period

Certificate Database

Confirmation

Progress

Results

Specify the cryptographic options

Select a cryptographic provider:
RSA#YubiHSM Key Storage Provider

Key length:
4096

Select the hash algorithm for signing certificates issued by this CA:

SHA256

SHA384

SHA512

SHA1

MD5

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

[More about Cryptography](#)

< Previous

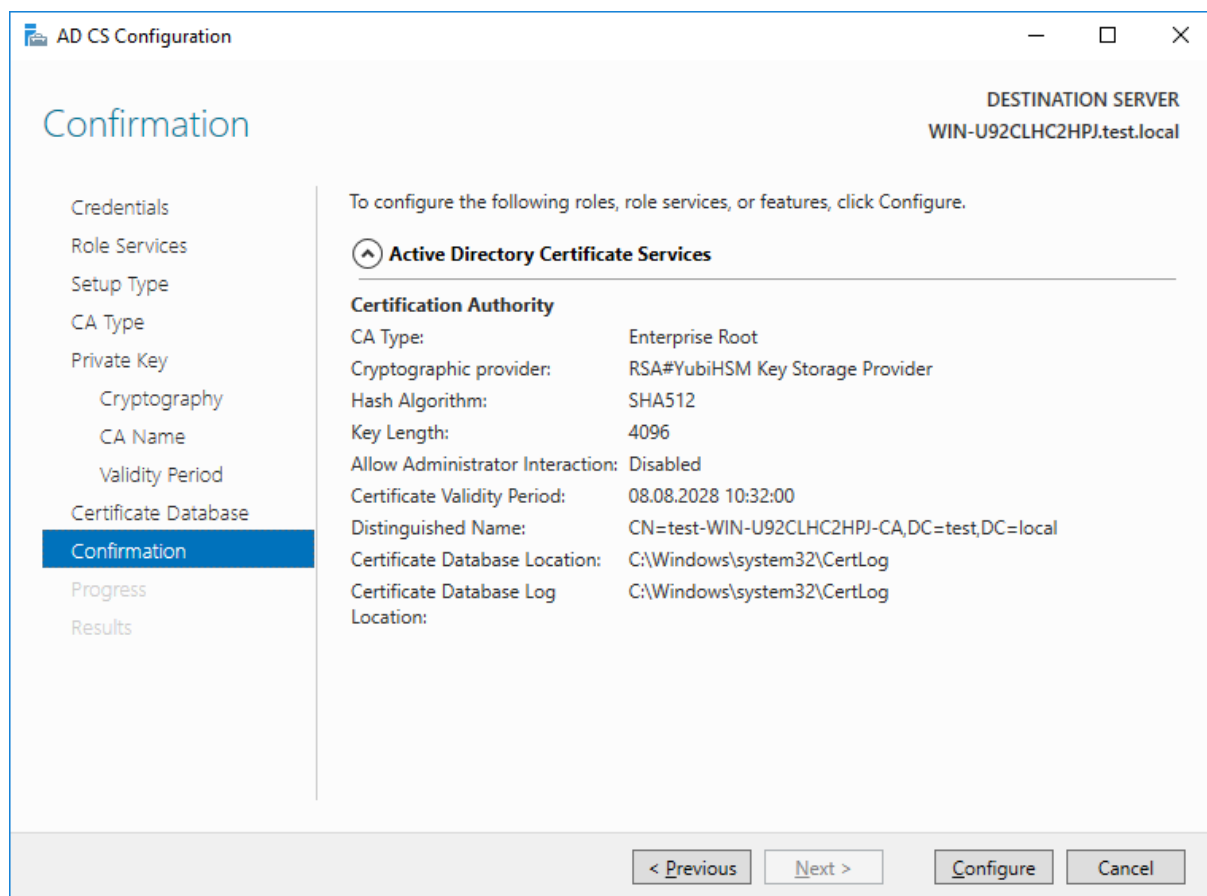
Next >

Configure

Cancel

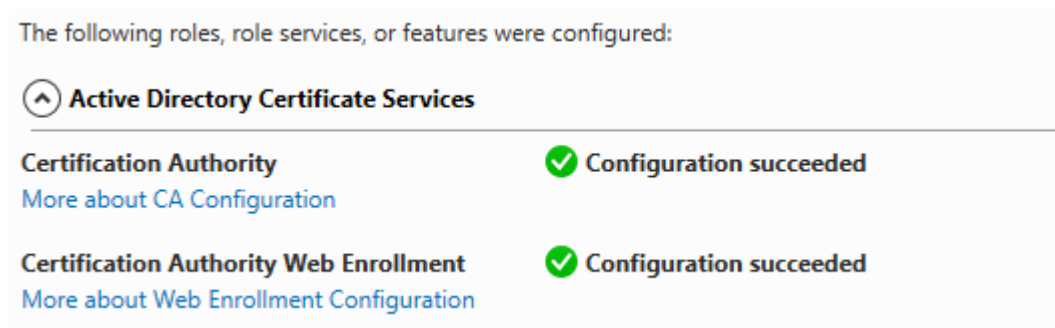
Select RSA#YubiHSM Key Storage Provider from the list displayed. This indicates that the root key should be generated on the YubiHSM.

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. If it did not work, go to the chapter [YubiHSM Troubleshooting](#).



The Active Directory Certificate Services and Certificate Authority Web Enrollment (<http://localhost/certsrv/>) are now ready for use.

If you are going to setup ACME, go to [ACME specific steps](#) for the CA server.

12.4 Migrate existing (root) CA certificate

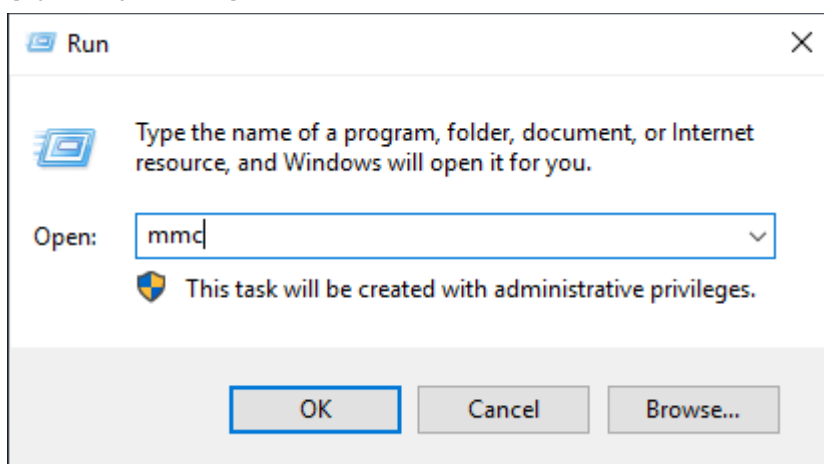


Please make sure that “Creating an application Authentication Key” is completed before proceeding. As shown in “Installing the YubiHSM Key Storage Provider”.

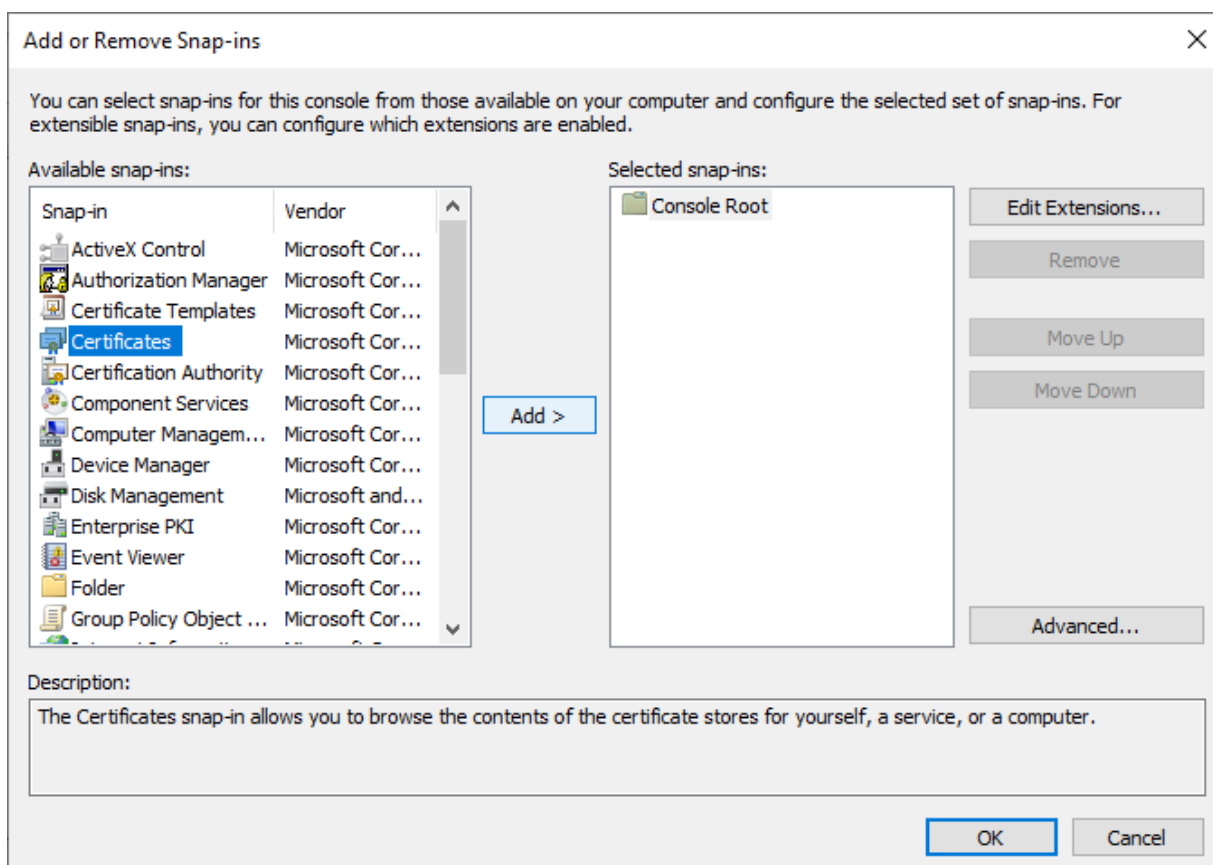
12.4.1 Export certificate to .pfx file

Create an MMC Snap-in for managing certificates on the Windows system where the SSL certificate is installed:

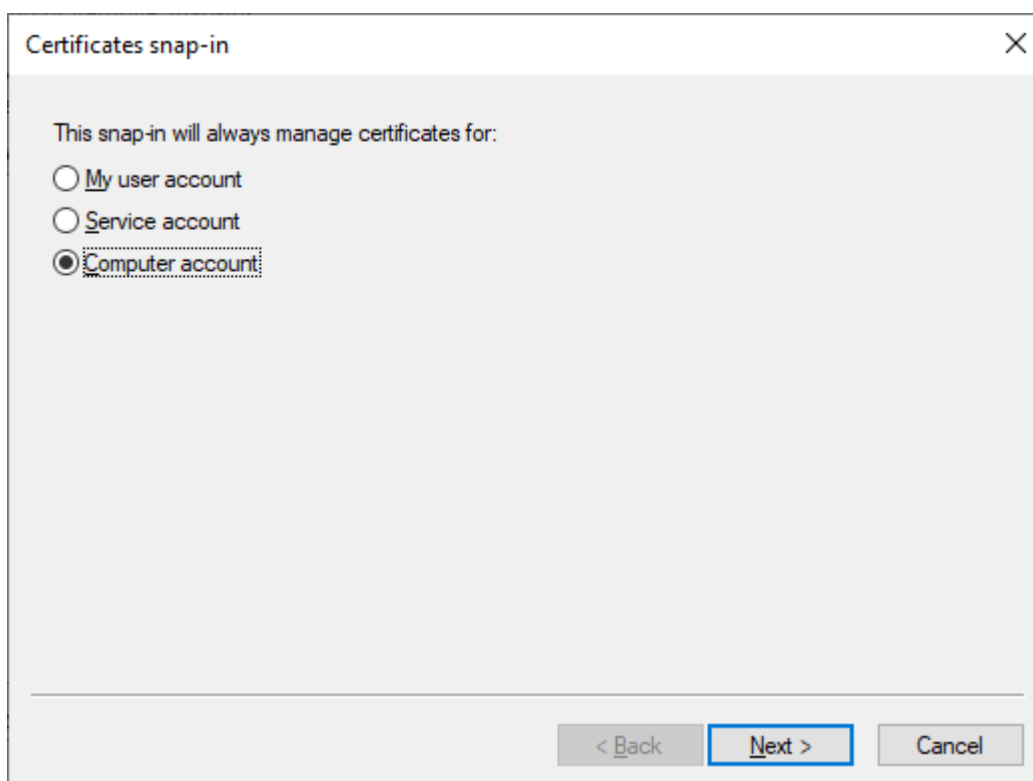
1. Start > run > MMC



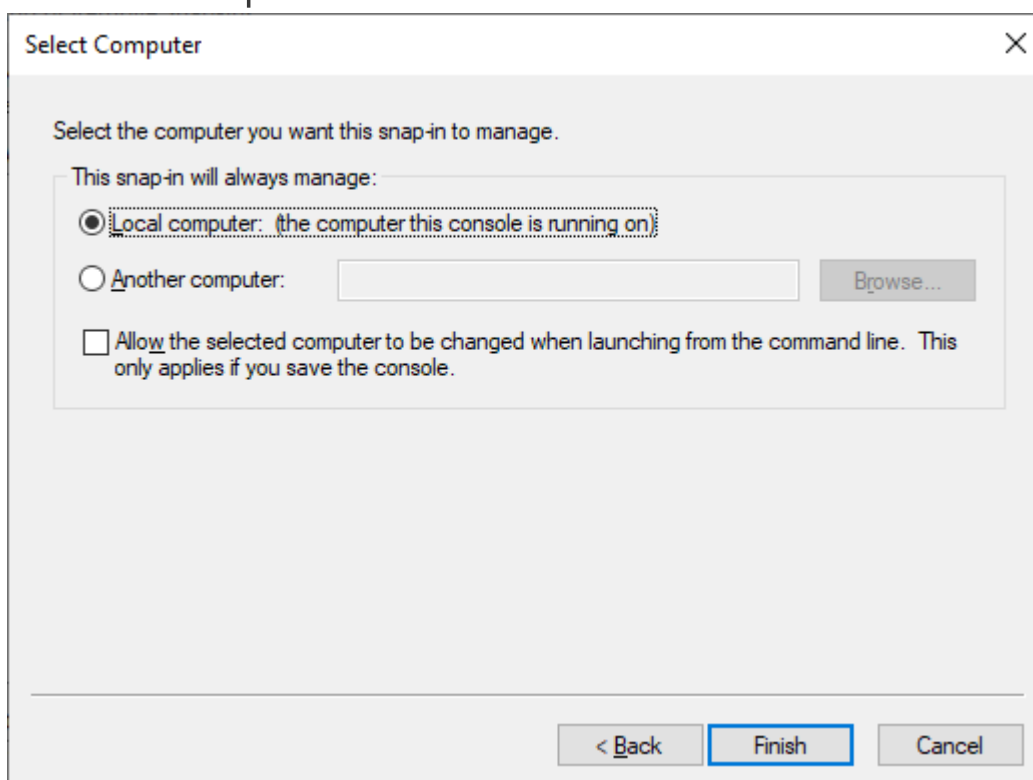
2. Go into the Console Tab > **File** > **Add/Remove Snap-in**.
3. Click on **Add** > Click on **Certificates** and click on **Add**.





4. Select **Computer Account** > **Next**.



5. Select **Local Computer > Finish**.



6. Close the **Add Standalone Snap-in** window.
7. Click on **OK** at the **Add/Remove Snap-in** window.
8. In MMC Double click on **Certificates (Local Computer)** in the center window.
9. Double click on the **Personal folder**, and then on **Certificates**.
10. Right Click on the Certificate you would like to backup and choose > **ALL TASKS > Export**
11. Follow the Certificate Export Wizard to backup your certificate to a .pfx file.

  Certificate Export Wizard

Welcome to the Certificate Export Wizard


This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

12. Select 'Yes, export the private key'

×

←  Certificate Export Wizard

Export Private Key
You can choose to export the private key with the certificate.

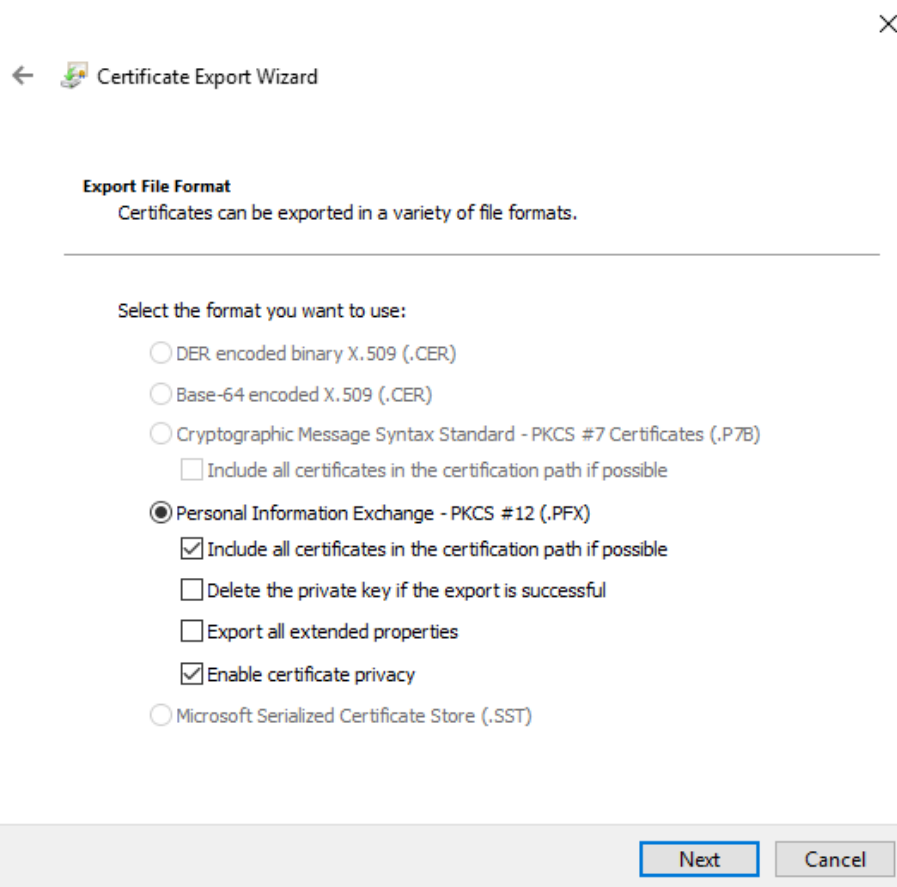
Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

Do you want to export the private key with the certificate?

☒ Yes, export the private key
☐ No, do not export the private key

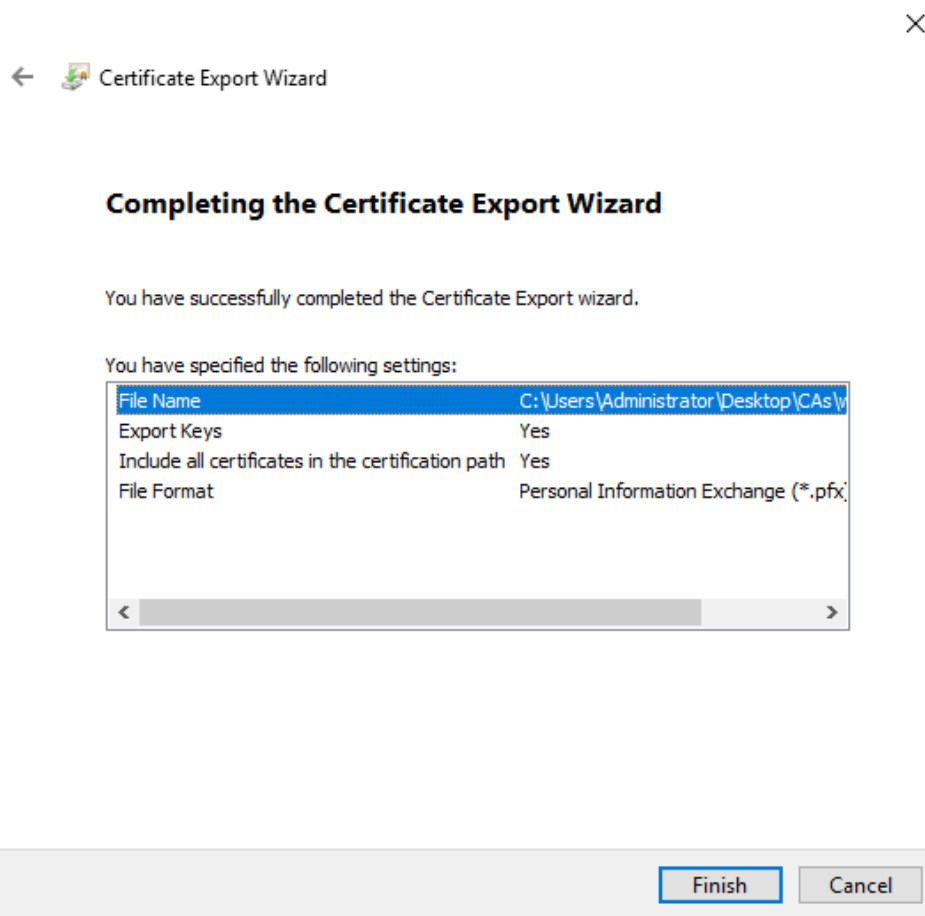
Next
Cancel

13. Select **"Include all certificates in certificate path if possible."** (do NOT select the delete Private Key option)



14. Enter a secure "PEM Password" and save it in a tool like a "Password Safe". You will need it in a later step.
15. Choose to save file on a set location.

16. Click **Finish**.

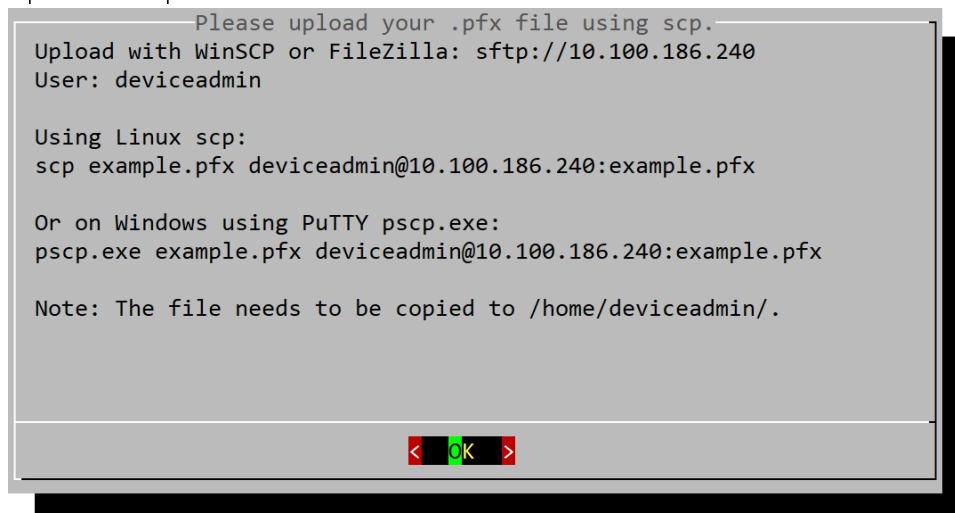


17. You will receive a message > “The export was successful.” > Click **OK**. The .pfx file backup is now saved in the location you selected and is ready to be moved or stored for your safe keeping.

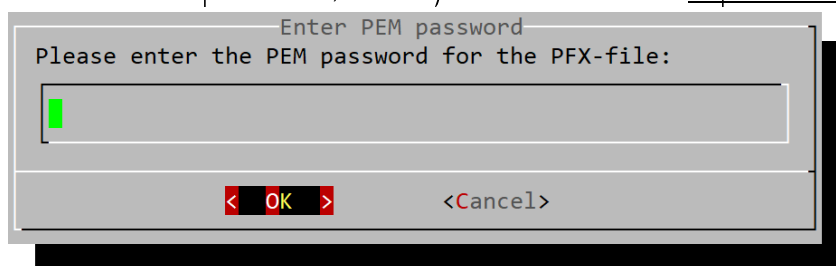
12.4.2 Import private key to YubiHSM

On the HSA go to: YubiHSM -> import

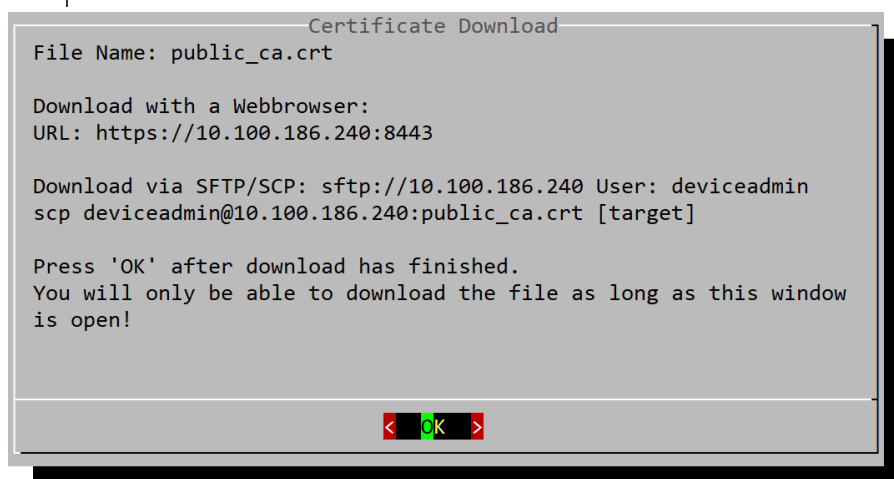
1. Enter the admin key password.
2. Upload the .pfx file to the HSA.



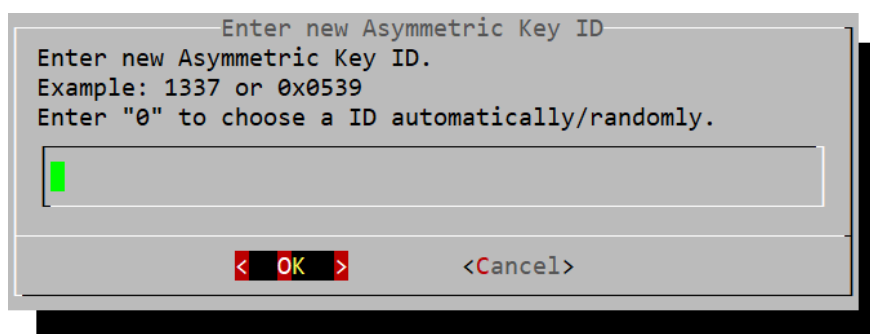
3. Enter the PEM password, which you have defined in Export certificate to .pfx file.



4. The public CA certificate can now be downloaded. You will need it in a later step.

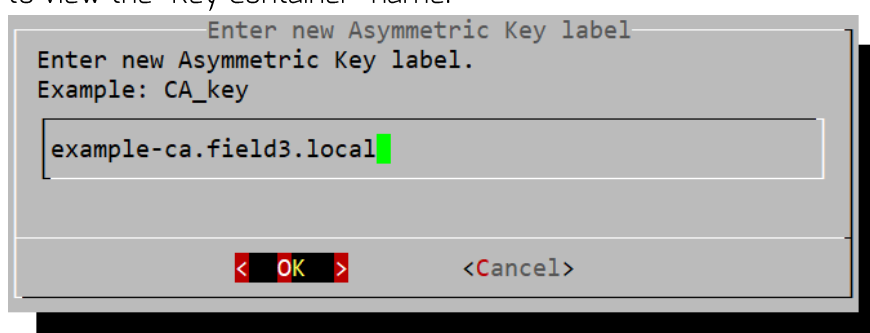


5. Enter a new key ID or press 0 to generate the ID automatically.

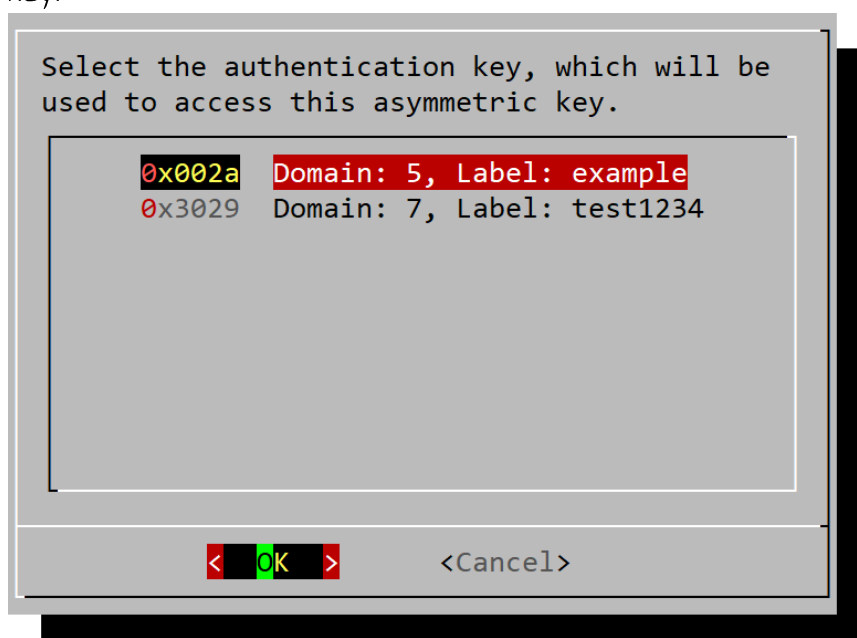


6. Enter a label to help identify the key.

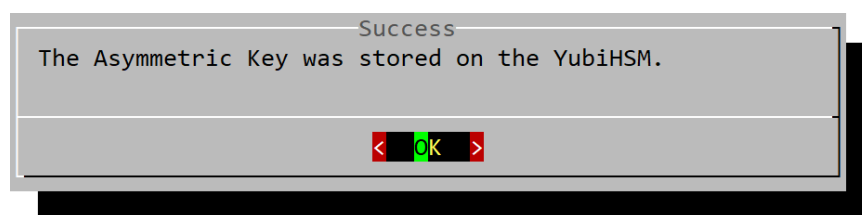
This should be the same name as it had in the old key storage provider. Otherwise, the repairstore command (in a later step) may fail. See [Decommission old Key Storage Provider](#) to view the "Key Container" name.



7. Select the domain and authentication key, which should be associated with this asymmetric key.



8. As soon as this window is visible, the generation process of the asymmetric key is finished.



12.4.3 Decommission old Key Storage Provider

Delete the original private key in your current provider. To do so, first execute:

```
#> certutil -store MY
```

```
PS C:\Users\Administrator> certutil -store MY
MY "Personal"
===== Certificate 0 =====
Serial Number: 23ffc8c90789f98a4be52681b328d07c
Issuer: CN=example-ca.field3.local, DC=field3, DC=local
NotBefore: 26.05.2021 13:10
NotAfter: 26.05.2041 13:20
Subject: CN=example-ca.field3.local, DC=field3, DC=local
Certificate Template Name (Certificate Type): CA
CA Version: V0.0
Signature matches Public Key
Root Certificate: Subject matches Issuer
Template: CA, Root Certification Authority
Cert Hash(sha1): 8b2557bd11e1724593e8816f77788283edd3d07f
Key Container = example-ca.field3.local
Unique container name: fa7a8a9bdb3d713dd505119fb67162bb_b53ca2dd-9218-4676-af02-ce18ceb544aa
Provider = Microsoft Software Key Storage Provider
Signature test passed
CertUtil: -store command completed successfully.
```

Locate the Cert Hash that corresponds with the CA

To actually delete the private key, execute:

```
#> cd cert:\localmachine\my
#> del -deletekey <Cert Hash>
```

Then stop the CA Service:

```
#> net stop CertSvc
```

Redirect the service to the YubiHSM module:

```
#> certutil -setreg CA\CSP\Provider "YubiHSM Key Storage Provider"
#> certutil -setreg CA\EncryptionCSP\Provider "YubiHSM Key Storage Provider"
```

12.4.4 Import certificate on CA


Import certificate (without key) into the certificate store:

```
#> certutil -addstore -f My <Certificate>
```


```
PS C:\Users\Administrator\Desktop\CAs> certutil -addstore -f My public_ca.crt
My "Personal"
Signature matches Public Key
Certificate "example-ca.field3.local" added to store.
CertUtil: -addstore command completed successfully.
PS C:\Users\Administrator\Desktop\CAs>
```


12.4.5 Registry Editor

Open the Registry Editor and navigate to

 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\<CA Name>\

and check that the following keys are set to *"YubiHSM Key Storage Provider"*:

 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\<CA Name>\CSP\Provider and

 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\<CA Name>\EncryptionCSP\Provider

12.4.6 Repair the Keystorage:

```
#> certutil -f -repairstore -csp "YubiHSM Key Storage Provider" MY <Hash>
```

Restart the Certificate Service:

```
#> net start CertSvc
```

When the certificate service starts, you have completed all steps correctly.

If you are going to setup ACME/EST go to [ACME/EST specific steps](#).

13 YubiHSM setup on a Linux CA

13.1 Linux CA Prerequisites

On the Linux CA you must install “yubihsm_pkcs11”. Therefore, visit <https://developers.yubico.com/YubiHSM2/Releases/> and download the package for your operating system. In our example, we will use the YubiHSM2-SDK for Debian12. Extract the archive with following command “`tar -xf yubihsm2-sdk-2023-11-debian12-amd64.tar.gz`”. Then go into the directory and install the .deb package for “yubihsm_pkcs11” with “`apt-get install ./package_name.deb`” (dependencies must also be installed).

13.2 Configuration on the YubiHSM

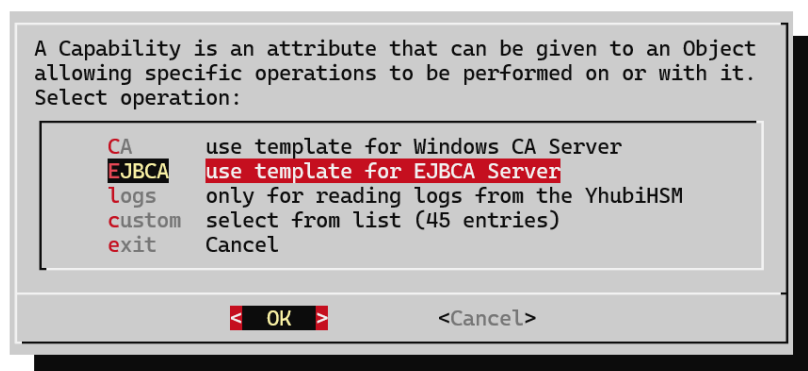
The following steps are required on the YubiHSM for use with a Linux CA.

13.2.1 YubiHSM default setup on the HSA

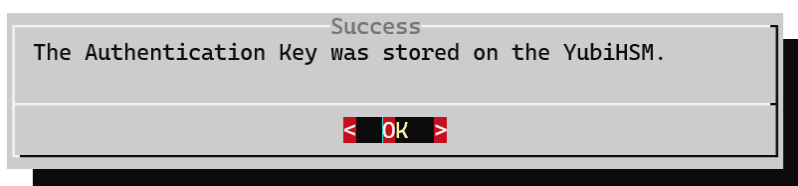
To run the YubiHSM setup on the HSA you must navigate to YubiHSM -> setup. Please note that this step **can be skipped** if it **has already been executed**.

13.2.2 Generate a new authentication key

Navigate to YubiHSM -> authenticationKey. Follow the authentication key creation until the selection of capabilities (see screenshot).



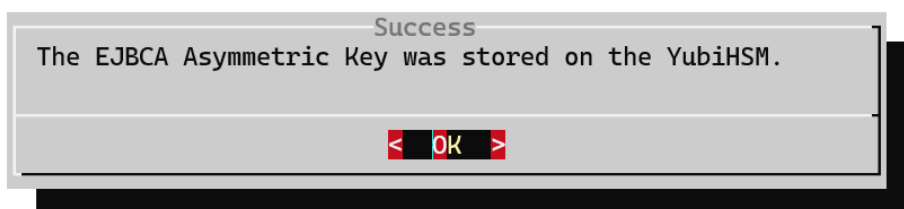
Select "EJBCA". You will then be prompted to enter the passphrase for the authentication key. Note that the passphrase must be at **least 8 characters long** so that the integration of the YubiHSM in your Linux CA succeeds. Then continue until you see the following below. The authentication key has been successfully created.



More detailed information on Authentication Key generation [here](#).

13.2.3 Generate an Asymmetric Key

To generate an asymmetric key for a Linux CA, go to YubiHSM->create. Then enter your admin key password. After that you will have to select an ID for your asymmetric key. Then you need to enter a key label. Next select the authentication you created and enter the passphrase for that key. Now it will take some time to create the asymmetric key. If it was successful, this message should be displayed.



More detailed information on Asymmetric Key generation [here](#).

13.3 Configuration on EJBCA

<https://docs.yubico.com/hardware/yubihsm-2/hsm-2-user-guide/webdocs.pdf#chapter.12>

Note: The YUBIHSM_PKCS11_CONF environment variable must be set in a start script of EJBCA.

13.4 Configuration on other CAs

For other CAs, refer to the chapter below and your CAs documentation.

<https://docs.yubico.com/hardware/yubihsm-2/hsm-2-user-guide/webdocs.pdf#chapter.10>

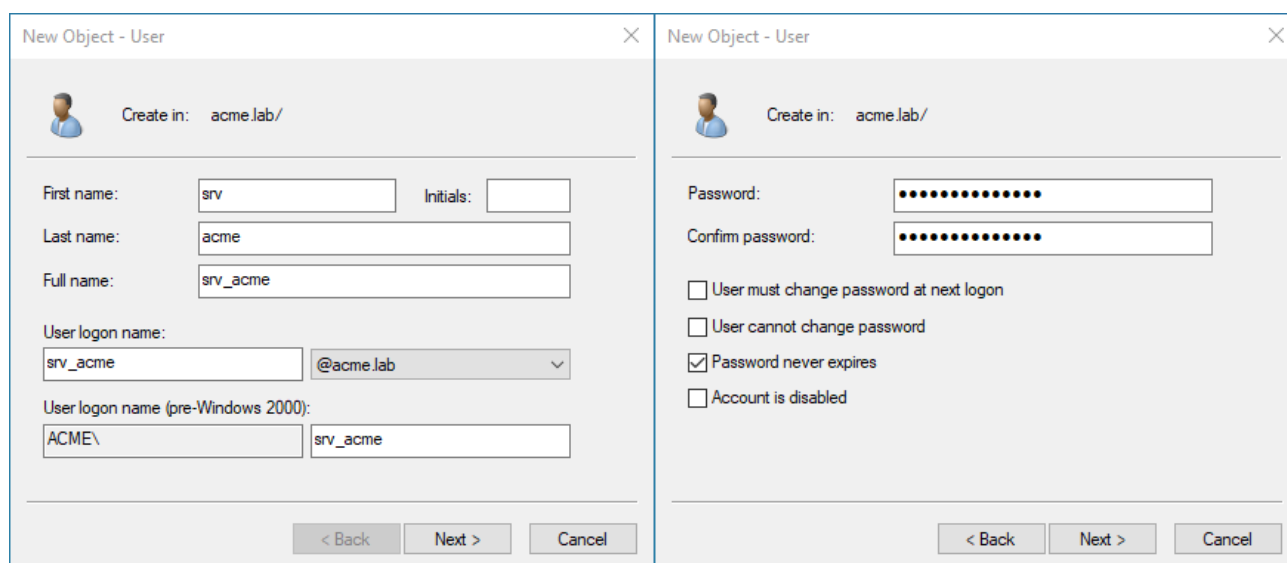
14 Setup CA for ACME/EST



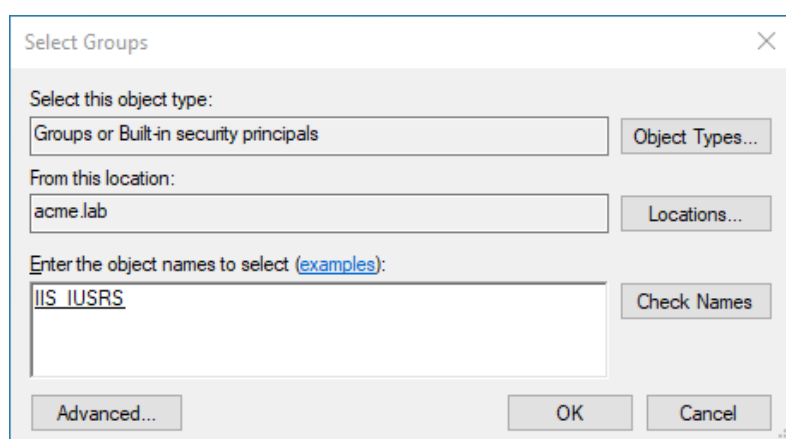
This guide assumes that a Windows CA has already been set up and is ready to use. If your CA setup is not complete, finish it and then continue here.

14.1 Creating Users for Authentication with the CA

To create a user open “Active Directory Users and Computers” → click on the root domain name → Users → right click on the free space → New → User



Once the user has been successfully created, right-click on the user and select 'Add to group...' (IIS_IUSRS).

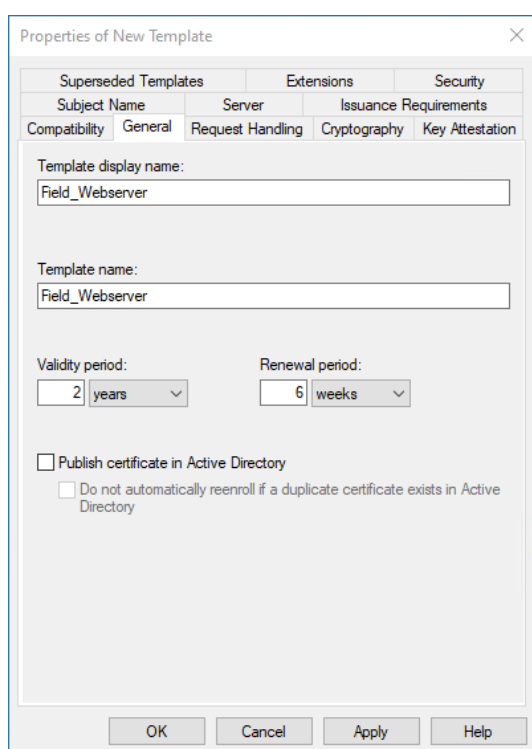


14.2 Creating a certificate template to issue

Now create a new certificate template to issue. This will be used when a certificate is enrolled with ACME or EST. Therefore, open "Certification Authority". Expand the dropdown → Right click on "Certificate Templates" → Manage → Right click on "Web Server" → Duplicate Template → Change some settings as described below

General:

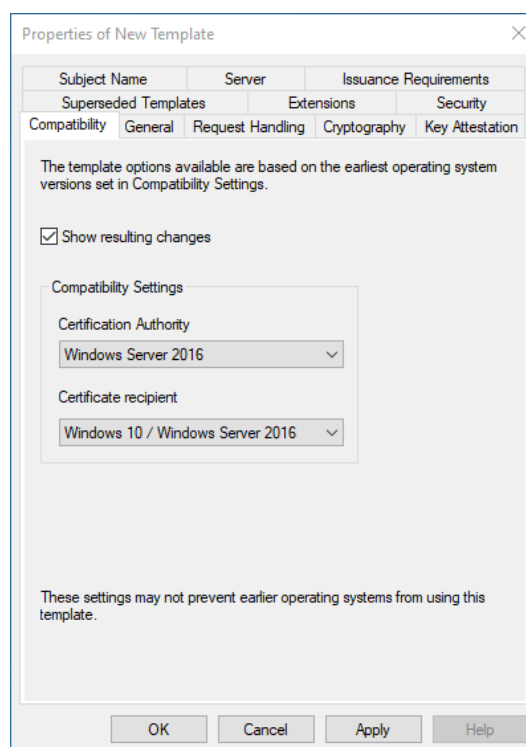
- Template display name/ Validity period/ Renewal period: to what you want



The screenshot shows the 'Properties of New Template' dialog box with the 'General' tab selected. The 'Superseded Templates' section is empty. The 'Subject Name' field is 'Field_Webserver'. The 'Template name' field is 'Field_Webserver'. The 'Validity period' is set to '2 years' and the 'Renewal period' is set to '6 weeks'. The 'Publish certificate in Active Directory' checkbox is unchecked, and the sub-option 'Do not automatically reenroll if a duplicate certificate exists in Active Directory' is also unchecked. The 'OK', 'Cancel', 'Apply', and 'Help' buttons are at the bottom.

Compatibility:

- Certification Authority: Windows Server 2016
- Certificate recipient: Windows 10 / Windows Server 2016



The screenshot shows the 'Properties of New Template' dialog box with the 'Compatibility' tab selected. The 'Subject Name' field is 'Field_Webserver'. The 'Template name' field is 'Field_Webserver'. The 'Validity period' is set to '2 years' and the 'Renewal period' is set to '6 weeks'. The 'Show resulting changes' checkbox is checked. The 'Compatibility Settings' section shows 'Certification Authority' set to 'Windows Server 2016' and 'Certificate recipient' set to 'Windows 10 / Windows Server 2016'. The 'OK', 'Cancel', 'Apply', and 'Help' buttons are at the bottom.

Cryptography:

- Provider Category: Key Storage Provider
- Minimum key size: 2048
- Request hash: SHA256 or higher

The screenshot shows the 'Properties of New Template' dialog box with the 'Cryptography' tab selected. The 'Provider Category' is set to 'Key Storage Provider', the 'Algorithm name' is 'RSA', and the 'Minimum key size' is '2048'. The 'Request hash' is set to 'SHA256'. The 'Use alternate signature format' checkbox is unchecked.

Security:

- Add the user you created and allow "enroll".

The screenshot shows the 'Properties of New Template' dialog box with the 'Security' tab selected. The 'Group or user names' list includes 'Authenticated Users', 'Administrator', 'Domain Admins (ACME\Domain Admins)', 'Enterprise Admins (ACME\Enterprise Admins)', and 'srv_acme (srv_acme@acme.lab)'. The 'Permissions for srv_acme' table shows 'Enroll' and 'Autoenroll' permissions set to 'Allow'.

Permissions for srv_acme	Allow	Deny
Full Control	<input type="checkbox"/>	<input type="checkbox"/>
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Write	<input type="checkbox"/>	<input type="checkbox"/>
Enroll	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Autoenroll	<input type="checkbox"/>	<input type="checkbox"/>

For EST to work, the following must also be configured in the certificate template.

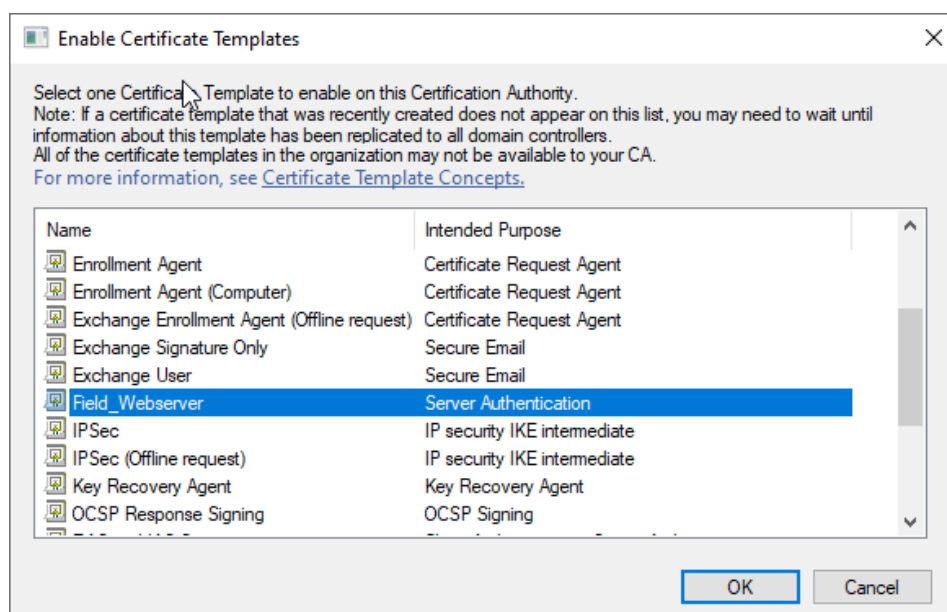
The screenshot shows the 'EST_IoT Properties' dialog box with the 'Extensions' tab selected. The 'Extensions included in this template' list includes 'Application Policies', 'Basic Constraints', 'Certificate Template Information', 'Issuance Policies', and 'Key Usage'. The 'Description of Application Policies' list includes 'Server Authentication' and 'Client Authentication'.

Extensions:

- Applications Policies: Add "Client Authentication"

When you are finished click on “Apply”.

In “Certification Authority”. Click on “Certificate Templates” → right click on the free space → New → Certificate Template to Issue → Select the template you have created before



14.3 Exporting the CA bundle

Finally, get the CA bundle. Therefore, export the certificate from each of your used CAs (Open “Certification Authority” → Right click on CA-name → Properties → General → View Certificate → Details → Copy to file → Base-64 encoded). Then combine the certificates into a single file by copy and pasting the file contents. Make sure the file extension is “.pem”. This file **is needed** for the setup of ACME/EST on the HSA.

14.4 Finishing touches

In order for ACME/EST to work, you will need to create DNS records for the clients and, if it is a cluster, also DNS records for the 2 nodes. Now you can continue with the ACME or EST setup on the HSA.

15 Let's Encrypt Mode for ACME

The Let's Encrypt Mode of the ACME Feature enables to proxy requests towards Let's Encrypt. This enables the retrieval of Let's Encrypt certificates within your internal network, without the need to expose all your systems to the internet.

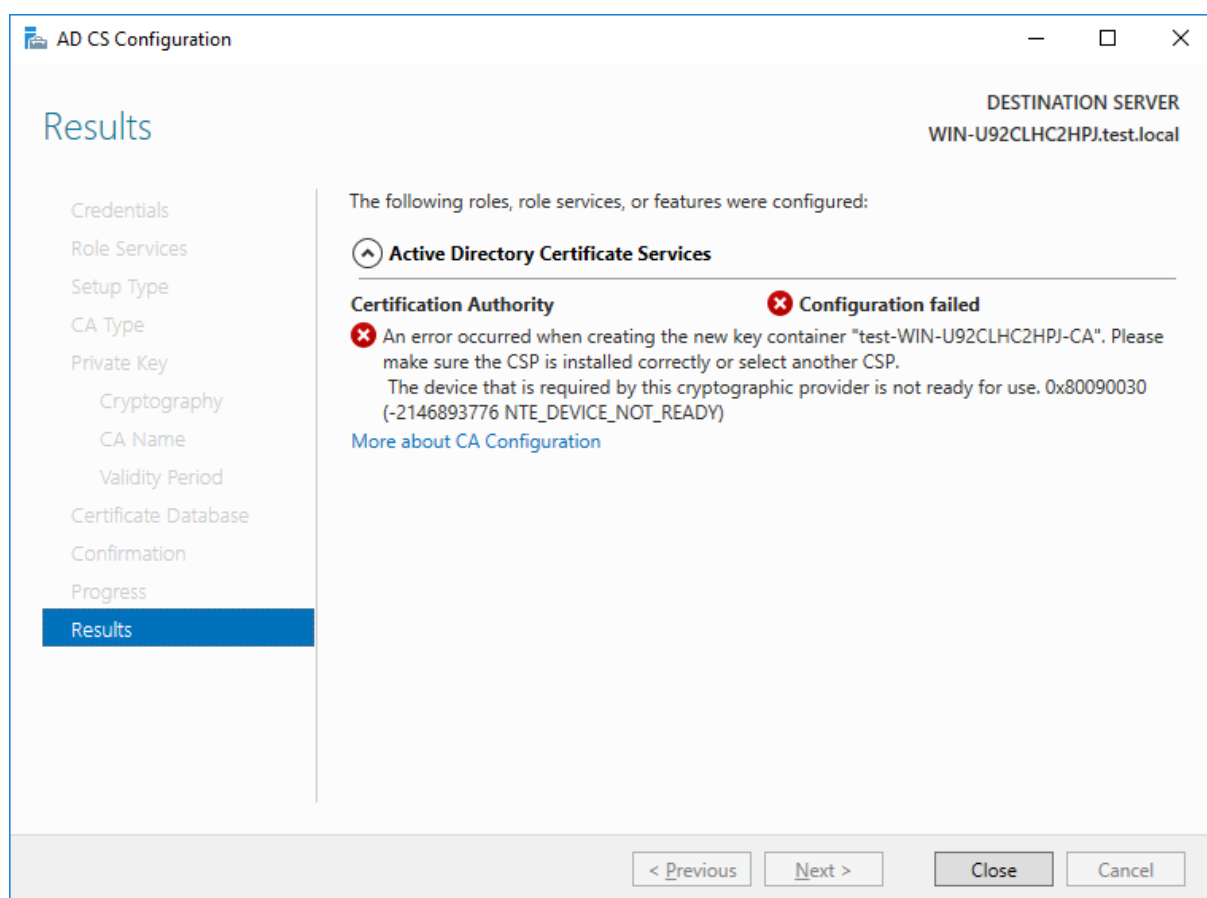
To use it for that, the following requirements must be met:

- The ACME container of your HSA must be reachable from the internet.

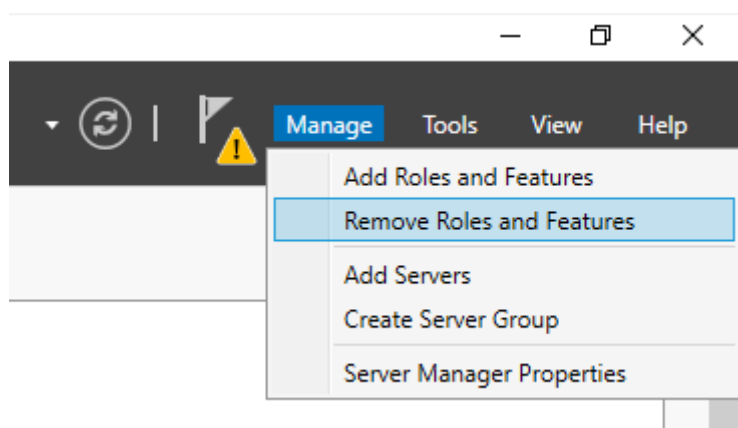
- The DNS domain you use internally must be official and you must own it.
- You will need to provide different sets of DNS information depending on the source address of the DNS query. Your internal clients and servers must resolve the addresses of your internal network, while external systems need to get the external address of the ACME container.

16 YubiHSM Troubleshooting

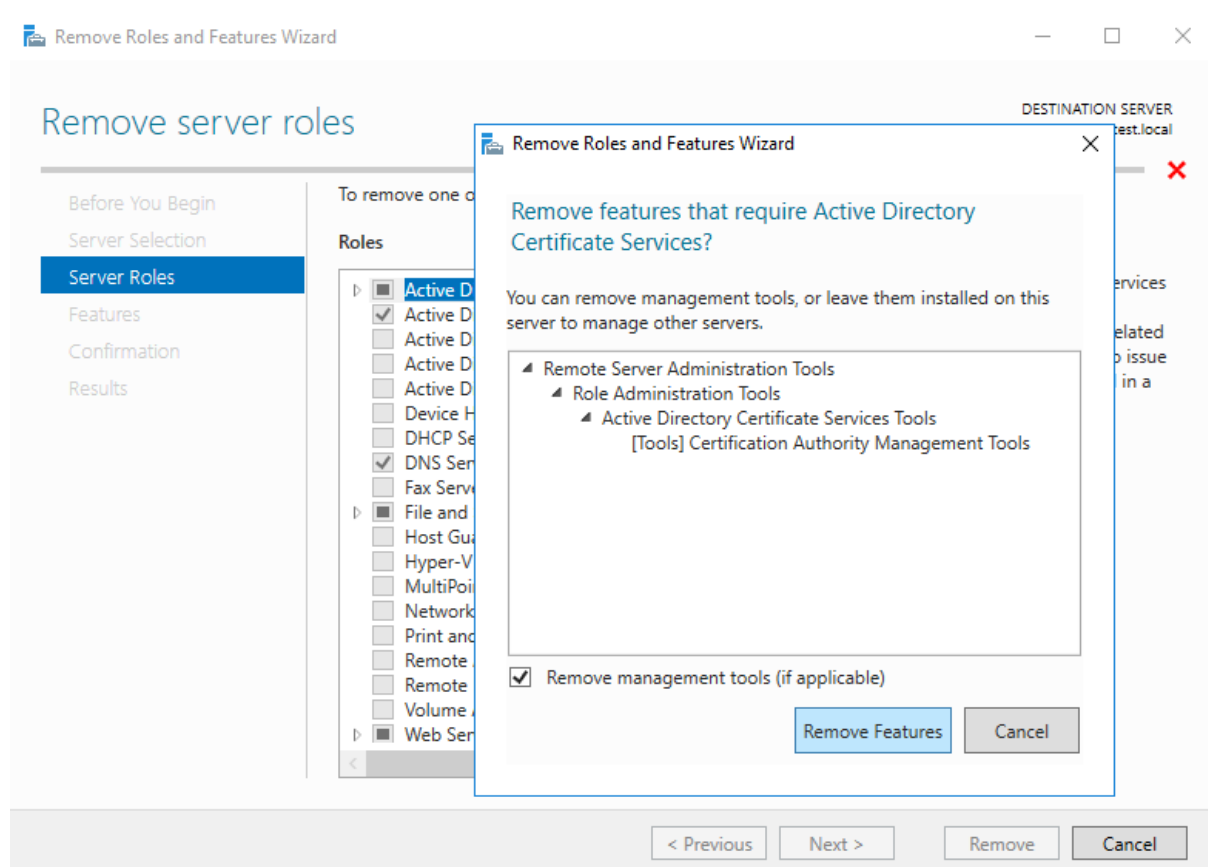
16.1 Active Directory Certificate Services



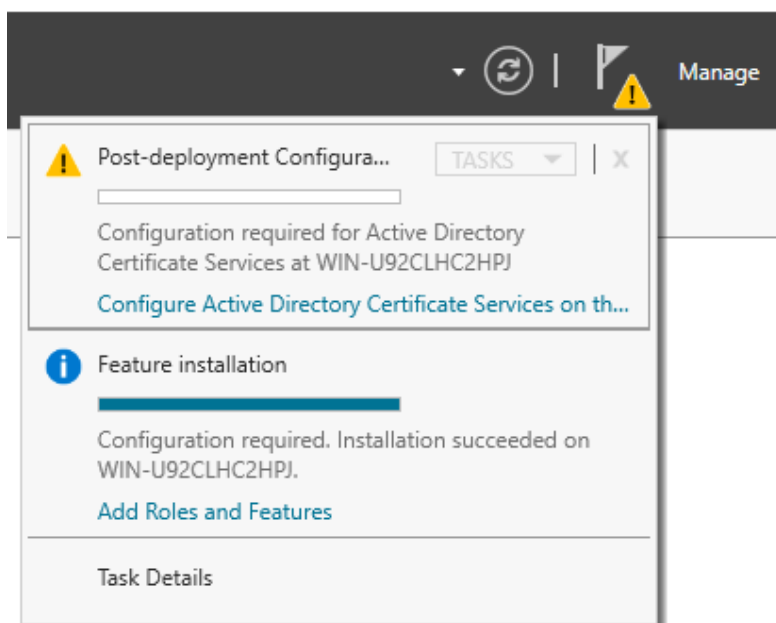
If you don't see "Configuration succeeded" but instead get the error "The device that is required by this cryptographic provider is not ready for use.", you can try this:



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

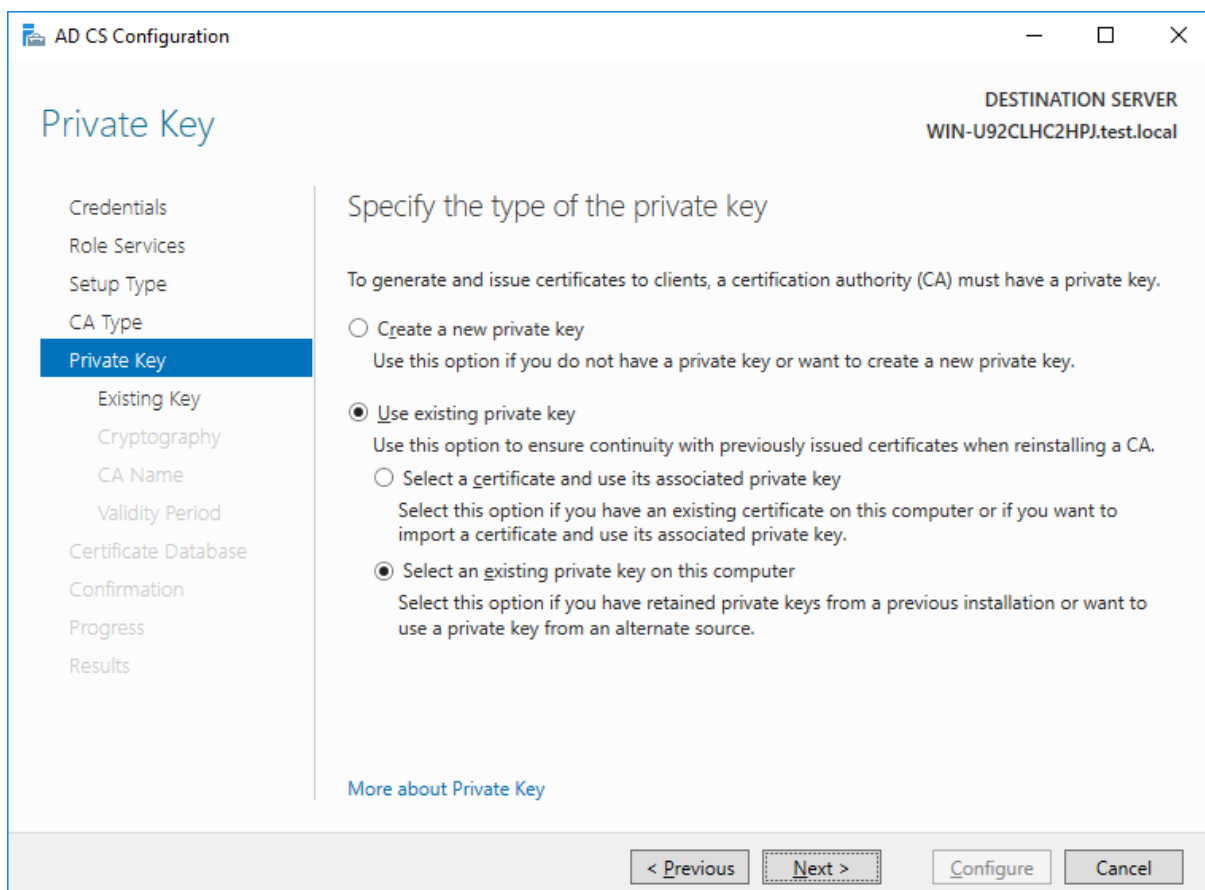


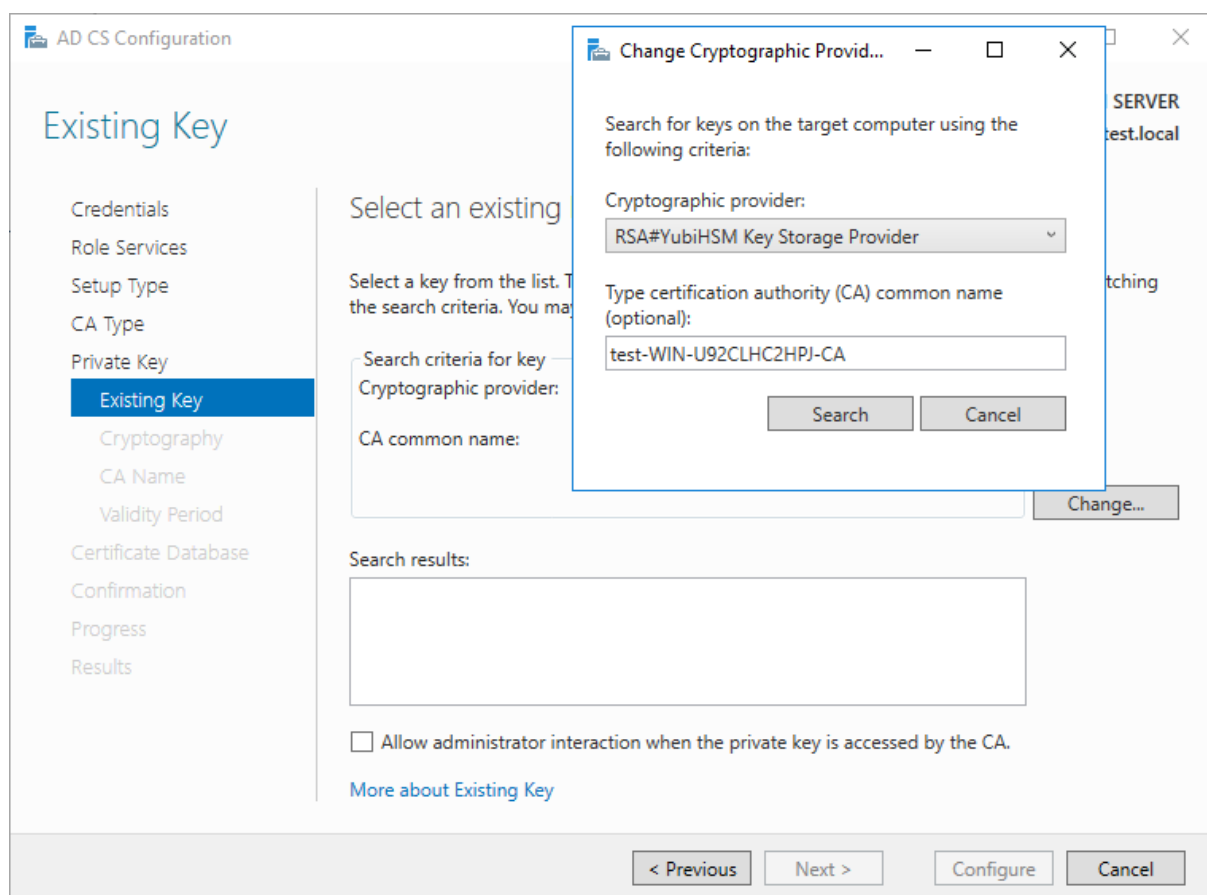
After reinstalling the Active Directory Certificate Services, start the configuration wizard again.



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 that the key was already created before but the wizard still reported “Configuration failed”.)

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





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

The screenshot shows the 'Existing Key' step of the AD CS Configuration wizard. The window title is 'AD CS Configuration'. On the left is a navigation pane with the following items: Credentials, Role Services, Setup Type, CA Type, Private Key, **Existing Key** (selected), Cryptography, CA Name, Validity Period, Certificate Database, Confirmation, Progress, and Results. The main area is titled 'Existing Key' and 'DESTINATION SERVER WIN-U92CLHC2HPJ.test.local'. It contains the instruction 'Select an existing key' and '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.' Below this is a 'Search criteria for key' box with 'Cryptographic provider: RSA#YubiHSM Key Storage Provider' and 'CA common name: test-WIN-U92CLHC2HPJ-CA'. A 'Change...' button is to the right. The 'Search results:' box contains one entry: 'test-WIN-U92CLHC2HPJ-CA'. At the bottom of the main area is a checkbox 'Allow administrator interaction when the private key is accessed by the CA.' and a link 'More about Existing Key'. The bottom of the window has four buttons: '< Previous', 'Next >', 'Configure', and 'Cancel'.

If you see a search result like [server name]-CA, then the private key was already created in the first attempt and you can use this key to complete the wizard.

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

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' and contains the following elements:

- DESTINATION SERVER:** WIN-U92CLHC2HPJ.test.local
- Instructions:** Select a hash algorithm for signing certificates issued by this certification authority (CA).
- Cryptographic provider:** A text box containing 'RSA#YubiHSM Key Storage Provider'.
- Hash algorithm:** A list box with the following options: SHA256, SHA384, SHA512 (which is currently selected), and SHA1.
- More about Cryptography:** A blue hyperlink at the bottom of the main area.
- Navigation buttons:** '< Previous', 'Next >', 'Configure', and 'Cancel' buttons are located at the bottom right of the window.

Proceed with the wizard, now the configuration should be successful.

The screenshot displays the configuration summary screen with the heading 'The following roles, role services, or features were configured:'. It lists the following components and their status:

- Active Directory Certificate Services** (indicated by an upward arrow icon):
 - Certification Authority:** Configuration succeeded (marked with a green checkmark). A link 'More about CA Configuration' is provided below.
 - Certification Authority Web Enrollment:** Configuration succeeded (marked with a green checkmark). A link 'More about Web Enrollment Configuration' is provided below.

17 ACME/EST Troubleshooting

If there is no networking issue, the normal log shows no meaningful message and the request does not work, it is recommended to enable the debug mode. To do this you can navigate from ACME or EST to configure -> debug and enable/disable the debug mode. You will then need to restart the corresponding container.

A common problem when requesting a certificate via ACME or EST is that the public key does not match the minimum size or algorithm required by the specified certificate template.

Example log snippet from the log menu option of ACME or EST:

Requesting certificate

Got error while trying to request certificate: code: 0x80094811 - CERTSRV_E_KEY_LENGTH - The public key does not meet the minimum size required by the specified certificate template.

Request ID is 157

This is also displayed on the CA.

	Request ID	Binary Request	Request Status Code	Request Disposition Message	Request Submission Date
acme-ACME-CA-CA	159	-----BEGIN NE...	The public key does not meet the minimum size required by the specified certificate template. 0x8...	Denied by Policy Module	24.09.2024 17:40
Revoked Certificates	158	-----BEGIN NE...	The public key does not meet the minimum size required by the specified certificate template. 0x8...	Denied by Policy Module	24.09.2024 17:40
Issued Certificates	157	-----BEGIN NE...	The public key does not meet the minimum size required by the specified certificate template. 0x8...	Denied by Policy Module	24.09.2024 17:40
Pending Requests					
Failed Requests					
Certificate Templates					

To resolve this issue, you can either change the key size/algorithm on the client side or change the requirements of the certificate template at your CA.