FINAL - PRE CEREMONY INITIALISATION 13/09/2018

Root Key Generation Ceremony - Act 0 initialise HSM

Anticipated Changes

- [x] Thomas Nicholson to add step to ensure that user information and residual CSLAN configuration has been removed 10 Sep 2018
- [x] Thomas Nicholson to add checksum information for OS and firmware versions 10 Sep 2018
- [ ] Thomas Nicholson to add attendees list **10 Sep 2018**
- [x] Thomas Nicholson to add signing space for IW confirming that OS and firmware matches checksums 10 Sep 2018
- [x] Thomas Nicholson to ensure subordinante HSM section matches root formatting

Prepare the root HSM

The CA carries out a reset on the root HSM to restore it to an "as shipped configuration", purge it of any residual cryptographic material and prepare it for the ceremony.

Approximate duration - 30 60 minutes.

Step	Activity	Initial	Time

0.1	**The CA demonstrates that the software images used to update the root HSM have the same fingerprint as those published by Utimaco.**
	CA Commentary: "I am now verifying that the HSM operating system and firmware images that I will update the HSM with match the checksums provided by the vendor"
	The following commands are carried out from the administration laptop
	`md5sum /path-to/SecurityServer-V4.21.0.3.zip`
	`checksum to match: 514aa0ef2a4a468890fc8f54b441005b`
	`md5sum /path-to/cslan-4.5.5.tar.gz`
	`checksum to match: 846c7955c49cb9f4e65a1e5a27410a31`
	[x] Thomas Nicholson to add anticipated output here
		WN	22:36

0.2	The CA Connects the administration laptop ethernet interface to the root HSM LON18-HSM01 CA Commentary: "I am now connecting the ethernet interface of the admin laptop to the root HSM"	WN	22:36

0.3 **If the device is factory fresh the CA will configure CSLAN, otherwise the CA will skip to step 0.4**

CA Commentary: "I am now configuring the ethernet interface of the HSM"

The following commands are carried out using the scroll buttons from the root HSM control panel.

1. The CA Configures CSLAN IP address:

   `CSLAN Administration -> Configuration -> Network -> IP Address -> IPv4 -> eth0`

   Set **192.168.4.203**

2. The CA disables CSLAN DHCP:

   `CSLAN Administration -> Configuration -> Network -> DHCP -> eth0`

3. The CA enables the SSH Daemon:

   `CSLAN Administration -> Configuration -> Services -> SSH Daemon -> Configuration`

   Set **192.168.4.0/24**

4. The CA set the boot partition to `user2`:

   `CSLAN Administration -> Update and Maintenance -> Set boot partition`

   set ```**user 2**```

5. The CA reboots the CSLAN:

   `CSLAN Administration -> Reboot`

6. The CA configures CSLAN IP address:

   `CSLAN Administration -> Configuration -> Network -> IP Address -> IPv4 -> eth0`

   Set **192.168.4.203**

7. Disable CSLAN DHCP:

   `CSLAN Administration -> Configuration -> Network -> DHCP -> eth0`

8. Enable SSH Daemon:

   `CSLAN Administration -> Configuration -> Services -> SSH Daemon -> Configuration`

   Set **192.168.4.0/24**

9. Reboot the CSLAN:

   `CSLAN Administration -> Reboot`

WN

0.4 **The CA Purges the Crypto Server via an External Erase**

CA Commentary: "I am now purging the HSM crypto server by carrying out an external erase"

1. The CA opens front panel door of the HSM and presses the ERASE CS button
2. The CA uses csadm to reset the Crypto server to factory default
   ./csadm Dev=192.168.4.203 Clear=Defaults
3. The CA resets the Alarm using csadmin and then restarts the Crypto server
   ./csadm Dev=192.168.4.203 LogonSign=Admin,key/ADMIN.key ResetAlarm
   /csadm Dev=192.168.4.203 Restart

Use name instead of IP WN

WN 22:41

↑ wrong path use full path WN

0.5 The CA resets the Alarm state on the HSM

CA Commentary: "I am now Loading the Firmware Modules for CryptoServer to bring the device to Operational Mode"

1. ./csadm Dev=192.168.4.203 LogonSign=Admin,key/ADMIN.key
   LoadPKG=/tcn/hsm/Firmware/SecurityServer-Se2-Series/SecurityServer-Se2-Series-4.21.0.3.mpkg
2. The CA waits until the HSM state returns to Operational on the front panel

full path = /tcn/hsm/key/ADMIN.key

WN

0.6 **The CA purges the HSM CSLAN**

CA Commentary: "I am now purging the HSM CSLAN"

The following commands are carried out using the scroll buttons from the root HSM control panel.

1. The CA switches the HSM to boot the CSLAN user1 partition from the HSM front panel:

   `CSLAN Administration -> Update and Maintenance -> Set boot partition`

   selects **user 1** partition

2. The CA Reboots the HSM:

   `CSLAN Administration -> Reboot`

3. The CA resets the CSLAN configuration:

   `CSLAN Administration -> Update and Maintenance -> Revert CSLAN Configuration`

   selects **yes** to confirm

4. The reboots the HSM:

   `CSLAN Administration -> Reboot`

5. The CA sets the boot partition to `user2`:

   `CSLAN Administration -> Update and Maintenance -> Set boot partition`

   selects user 2

6. The CA Reboot the HSM:

   `CSLAN Administration -> Reboot`

7. Reset the CSLAN configuration:

   `CSLAN Administration -> Update and Maintenance -> Revert CSLAN Configuration`

   selects **yes**

8. The CA reboots the HSM:

   `CSLAN Administration -> Reboot`

9. The CA sets the boot partition to `user1`:

   `CSLAN Administration -> Update and Maintenance -> Set boot partition`

   selects user 1

10. The CA reboots the CSLAN:

    `CSLAN Administration -> Reboot`

0.7 **CA configures CS LAN**

CA Commentary: "I am now configuring the HSM CSLAN ethernet interface as it has now been reset"

The following commands are carried out using the scroll buttons from the root HSM control panel.

Initial configuration will be for user 1 partition

1. The CA Configures CSLAN IP address:

   `CSLAN Administration -> Configuration -> Network -> IP Address -> IPv4 -> eth0`

   Set 192.168.4.203/24, selects ```yes``` to accept

2. The CA disables CSLAN DHCP:

   `CSLAN Administration -> Configuration -> Network -> DHCP -> eth0`

   selects disabled already disabled WN

3. The CA enables the SSH Daemon:

   `CSLAN Administration -> Configuration -> Services -> SSH Daemon -> Configuration`

   selects **yes** to enable. and OK to allow default range (it's own prefix).

4. The CA set the boot partition to `user2`:

   `CSLAN Administration -> Update and Maintenance -> Set boot partition`

   selects ```**user 2**```

5. The CA reboots the CSLAN:

   `CSLAN Administration -> Reboot`

The CA will then configure CSLAN for the user 2 partition

1. The CA configures CSLAN IP address:

   `CSLAN Administration -> Configuration -> Network -> IP Address -> IPv4 -> eth0`

   Set **192.168.4.203** selects ```**yes**``` **to accept**

2. The CA disables the CSlan DHCP:

   `CSLAN Administration -> Configuration -> Network -> DHCP -> eth0`

   selects ```disabled``` already disabled WN

3. The CA enables the SSH Daemon:

   `CSLAN Administration -> Configuration -> Services -> SSH Daemon -> Configuration`

   selects ```**yes**``` to enable. and ```OK``` to allow default range (it's own prefix).

4. The CA set the boot partition to `user1`:

   `CSLAN Administration -> Update and Maintenance -> Set boot partition`

   selects **user 1**

5. The CA Reboots the CSLAN:

   `CSLAN Administration -> Reboot`

WN 22.55

0.8 **The CA Configures CS Logging**

CA Commentary: "I am now enabling and confirming audit logging on the HSM"

The following commands are carried out from the administration laptop.

The CA sets Audit Log settings (via the administration user interface) so that all event types are logged.

1. The CA sets Audit Log settings so that all event types are logged. (the command will silently succeed)

   ```
   csadm Dev=192.168.4.203 LogonSign=ADMIN,key/ADMIN.key SetAuditConfig=Events=0x00000007
   ```

2. The CA verifies the audit log settings: (expected output):

   csadm Dev=192.168.4.203 LogonSign=ADMIN,key/ADMIN.key GetAuditConfig
   Audit log configuration parameters:
   Number of logfiles: 3
   Rotate logfiles: yes
   Max filesize: 200000
   Events: 0x00000007 (Bits 1:2:3)

0.9 **The CA updates the operating system of the CryptoServer LAN.**

CA Commentary: "I am now upgrading the CryptoServer LAN (CSLAN) software"

Note that unlike the configuration changes, these steps will update the *inactive* partition, therefore, if "user 1" is the active partition, the OS update will run against "user 2". These steps therefore use the getBoot.sh command to determine the active partition and to indicate the appropriate partition to boot into to ensure the allow changing to ensure the OS is updated across both boot partitions

The following commands are carried out from the administration laptop.

The CA updates the operating system in the first boot partition

1. The CA Uploads the CSLanOS file via SCP to HSM using the default Utimaco cslagent password

   ```
   scp cslan-4.5.5.tar.gz cslagent@192.168.4.203:/home/cslagent/
   ```

2. The CA logs into the CryptoServer LAN as the cslagent user via SSH using the default cslagent password

   ```
   ssh 192.168.4.203 -l cslagent
   su -l
   ```
   (the CA supplies the default cslagent password)

3. The CA runs the update script with the new cslan-4.5.5.tar.gz file:

   ```
   update.sh /home/cslagent/cslan-4.5.5.tar.gz
   ```

4. The CA checks which partition is booted using the getBoot.sh tool

   ```
   getBoot.sh
   ```

   This will return either 1 or 2. The previous command will have updated the inactive partition.

5. The CAs the boot partition you just updated to be started after reboot:

   ```
   setBoot.sh usern
   ```

   (where n is the partition number of the inactive partition)

6. The CA reboots the CryptoServer LAN into the inactive partion

   ```
   reboot
   ```

The CA updates the operating system in the second boot partition

1. **The CA checks that the inactive partition has the expected version:**

   ```
   csadm Dev=192.168.4.203 CSLGetVersion
   ```

   Expect 4.5.5

2. The CA logs into the CryptoServer LAN as the cslagent user via SSH

   ```
   ssh 192.168.4.203 -l cslagent
   su -l
   ```
   (the CA supplies the default cslagent password)

   Used alternative ssh comma WN

3. The CA runs the update script with the new cslan-4.5.5.tar.gz file:

   ```
   update.sh /home/cslagent/cslan-4.5.5.tar.gz
   ```

4. The CA checks which partition is booted using the getBoot.sh tool

   ```
   getBoot.sh
   ```

   This will return either 1 or 2. The previous command will have updated the inactive partition.

   WN 22:58

5. The CAs the boot partition you just updated to be started after reboot:

   ```
   setBoot.sh usern
   ```

   (where n is the partition number of the inactive partition)

6. The CA reboots the CryptoServer LAN into the inactive partion

   ```
   reboot
   ```

7. **The CA checks that the inactive partition has the expected version:**

   ```
   csadm Dev=192.168.4.203 CSLGetVersion
   ```

   Expect 4.5.5

0.10 **The CA lists CryptoServer Firmware Modules**

CA Commentary: "These are the Firmware modules loaded a part of the Crypto Server clear process"
./csadmn Dev=192.168.4.203 ListFirmware

Expect:

ID name type version initialization level
---
0 SMOS C64 5.5.9.1 INIT_OK
4 POST C64 1.0.0.2 INIT_OK
a HCE C64 2.2.2.3 INIT_INACTIVE
d EXAR C64 2.2.1.1 INIT_INACTIVE
68 CXI C64 2.3.0.5 INIT_OK
81 VDES C64 1.0.9.3 INIT_OK
82 PP C64 1.3.1.7 INIT_OK
83 CMDS C64 3.6.2.0 INIT_OK
84 VRSA C64 1.3.6.1 INIT_OK
85 SC C64 1.2.0.3 INIT_OK
86 UTIL C64 3.0.5.1 INIT_OK
87 ADM C64 3.0.25.5 INIT_OK
88 DB C64 1.3.2.2 INIT_OK
89 HASH C64 1.0.11.2 INIT_OK
8b AES C64 1.4.1.4 INIT_OK
8d DSA C64 1.2.3.3 INIT_OK
8e LNA C64 1.2.4.2 INIT_OK
8f ECA C64 1.1.12.4 INIT_OK
91 ASN1 C64 1.0.3.6 INIT_OK
96 MBK C64 2.2.8.2 INIT_OK
9a NTP C64 1.2.0.9 INIT_OK
9c ECDSA C64 1.1.16.1 INIT_OK

WN 23:01

0.11 CA Commentary: "The root HSM has now been purged and the CSLAN and firmware images have been updated to the latest versions"

WN 23:01

0.12 CA Commentary "The only existing user is the default admin"

The CA present the list of users
csadm Dev=192.168.4.203 ListUser
expect only default ADMIN user, if not re-purge

WN 23:02

We tried to synchronize time at this point WN

Prepare the subordinate HSM

The CA carries out a reset on the subordinate HSM to restore it to an "as shipped configuration" and purge it of any residual cryptographic material.

Approximate duration - 30 60 minutes.

Step	Activity	Initial	Time
0.13	The CA Connects the administration laptop ethernet interface to the root HSM LON18-HSM01 CA Commentary: "I am now connecting the ethernet interface of the admin laptop to the subordinate HSM"		

0.14	**If the device is factory fresh the CA will configure CSLAN, otherwise the CA will skip to step 0.15**
	CA Commentary: "I am now configuring the ethernet interface of the HSM"
	The following commands are carried out using the scroll buttons from the root HSM control panel.
	1. The CA Configures CSLAN IP address:
	`CSLAN Administration -> Configuration -> Network -> IP Address -> IPv4 -> eth0`
	Set **192.168.4.204**
	2. The CA disables CSLAN DHCP:
	`CSLAN Administration -> Configuration -> Network -> DHCP -> eth0`
	3. The CA enables the SSH Daemon:
	`CSLAN Administration -> Configuration -> Services -> SSH Daemon -> Configuration`
	Set **192.168.4.0/24**
	4. The CA set the boot partition to `user2`:
	`CSLAN Administration -> Update and Maintenance -> Set boot partition`
	set ```**user 2**```
	5. The CA reboots the CSLAN:
	`CSLAN Administration -> Reboot`
	6. The CA configures CSLAN IP address:
	`CSLAN Administration -> Configuration -> Network -> IP Address -> IPv4 -> eth0`
	Set **192.168.4.204**
	7. Disable CSLAN DHCP:
	`CSLAN Administration -> Configuration -> Network -> DHCP -> eth0`
	8. Enable SSH Daemon:
	`CSLAN Administration -> Configuration -> Services -> SSH Daemon -> Configuration`
	Set **192.168.4.0/24**
	9. Reboot the CSLAN:
	`CSLAN Administration -> Reboot`
		WJ 23:08
		Skip	

0.15 **The CA Purges the Crypto Server via an External Erase**

CA Commentary: "I am now purging the HSM crypto server by carrying out an external erase"

The following commands are carried out using the scroll buttons from the root HSM control panel.

1. The CA opens front panel door of the HSM and presses the ERASE CS button
2. The CA uses csadm to reset the Crypto server to factory default
   ./csadm Dev=192.168.4.204 Clear=Defaults
3. The CA resets the Alarm using csadmin and then restarts the Crypto server
   ./csadm Dev=192.168.4.204 LogonSign=Admin,key/ADMIN.key ResetAlarm
   /csadm Dev=192.168.4.204 Restart

The CS locked up and CA power cycle it WN 23:12

full path WN

Used hostname rather than IP WN

0.16 The CA resets the Alarm state on the HSM

CA Commentary: "I am now resetting the HSM from its alarm state"

The following commands are carried out from the administration laptop

1. On the administration laptop the CA types the following:

```
cd /tcn/hsm/Software/Linux/x86-64/Administration
./csadm Dev=192.168.4.204 LogonSign=ADMIN,key/ADMIN.key ResetAlarm
./csadm Dev=192.168.4.204 Restart
./csadm Dev=192.168.4.204 LogonSign=Admin,key/ADMIN.key
LoadPKG=/tcn/hsm/SecurityServer-Se2-Series-4.21.0.3.mpkg
```

2. The CA waits until the HSM state returns to Operational on the front panel

repeat of point 0.15 WN

WN 23:14

this command was involved

0.17 **The CA purges the HSM CSLAN**

CA Commentary: "I am now purging the HSM CSLAN"

The following commands are carried out using the scroll buttons from the root HSM control panel.

1. The CA switches the HSM to boot the CSLAN user1 partition from the HSM front panel:

   `CSLAN Administration -> Update and Maintenance -> Set boot partition`

   selects **user 1** partition

2. The CA Reboots the HSM:

   no need to reboot WN

   `CSLAN Administration -> Reboot`

3. The CA resets the CSLAN configuration:

   `CSLAN Administration -> Update and Maintenance -> Revert CSLAN Configuration`

   selects **yes** to confirm

4. The reboots the HSM:

   `CSLAN Administration -> Reboot`

5. The CA sets the boot partition to `user2`:

   `CSLAN Administration -> Update and Maintenance -> Set boot partition`

   selects user 2

   WN 23:20

6. The CA Reboot the HSM:

   `CSLAN Administration -> Reboot`

7. Reset the CSLAN configuration:

   `CSLAN Administration -> Update and Maintenance -> Revert CSLAN Configuration`

   selects **yes**

8. The CA reboots the HSM:

   `CSLAN Administration -> Reboot`

9. The CA sets the boot partition to `user1`:

   `CSLAN Administration -> Update and Maintenance -> Set boot partition`

   selects user 1

10. The CA reboots the CSLAN:

    `CSLAN Administration -> Reboot`

0.18 **CA configures CS LAN**

CA Commentary: "I am now configuring the HSM CSLAN ethernet interface as it has now been reset"

The following commands are carried out using the scroll buttons from the root HSM control panel.

Initial configuration will be for user 1 partition

1. The CA Configures CSLAN IP address:

   `CSLAN Administration -> Configuration -> Network -> IP Address -> IPv4 -> eth0`

   Set **192.168.4.204/24**, selects ```**yes**``` to accept

2. The CA disables CSLAN DHCP:

   `CSLAN Administration -> Configuration -> Network -> DHCP -> eth0`

   selects disabled disabled already WN

3. The CA enables the SSH Daemon:

   `CSLAN Administration -> Configuration -> Services -> SSH Daemon -> Configuration`

   selects **yes** to enable, and OK to allow default range (it's own prefix).

4. The CA set the boot partition to `user2`:

   `CSLAN Administration -> Update and Maintenance -> Set boot partition`

   selects ```**user 2**```

   WN 23.26

5. The CA reboots the CSLAN:

   `CSLAN Administration -> Reboot`

The CA will then configure CSLAN for the user 2 partition

1. The CA configures CSLAN IP address:

   `CSLAN Administration -> Configuration -> Network -> IP Address -> IPv4 -> eth0`

   Set **192.168.4.204** selects ```**yes**``` **to accept**

2. The CA disables the CSlan DHCP:

   `CSLAN Administration -> Configuration -> Network -> DHCP -> eth0`

   selects ```disabled``` disabled already WN

3. The CA enables the SSH Daemon:

   `CSLAN Administration -> Configuration -> Services -> SSH Daemon -> Configuration`

   selects ```**yes**``` to enable, and ```OK``` to allow default range (it's own prefix).

4. The CA set the boot partition to `user1`:

   `CSLAN Administration -> Update and Maintenance -> Set boot partition`

   selects **user 1**

5. The CA Reboots the CSLAN:

   `CSLAN Administration -> Reboot`

0.19 **The CA Configures CS Logging**

CA Commentary: "I am now enabling and confirming audit logging on the HSM"

The following commands are carried out from the administration laptop.

The CA sets Audit Log settings (via the administration user interface) so that all event types are logged.

1. The CA sets Audit Log settings so that all event types are logged. (the command will silently succeed)

   ```
   csadm Dev=192.168.4.204 LogonSign=ADMIN,key/ADMIN.key SetAuditConfig=Events=0x00000007
   ```

   LN 23:26

2. The CA verifies the audit log settings: (expected output): Used full path LN

   csadm Dev=192.168.4.204 LogonSign=ADMIN,key/ADMIN.key GetAuditConfig
   Audit log configuration parameters:
   Number of logfiles: 3
   Rotate logfiles: yes
   Max filesize: 200000
   Events: 0x00000007 (Bits 1:2:3)

0.20 **The CA updates the operating system of the CryptoServer LAN.**

CA Commentary: "I am now upgrading the CryptoServer LAN (CSLAN) software"

Note that unlike the configuration changes, these steps will update the *inactive* partition, therefore, if "user 1" is the active partition, the OS update will run against "user 2". These steps therefore use the getBoot.sh command to determine the active partition and to indicate the appropriate partition to boot into to ensure the OS is updated across both boot partitions

The following commands are carried out from the administration laptop.

The CA updates the operating system in the first boot partition

1. The CA Uploads the CSLanOS file via SCP to HSM using the default Utimaco cslagent password

   scp cslan-4.5.5.tar.gz cslagent@192.168.4.204:/home/cslagent
2. The CA logs into the CryptoServer LAN as the cslagent user via SSH using the default cslagent password

   ```
   ssh 192.168.4.204 -l cslagent
   su -l
   ```
   (the CA supplies the default cslagent password)

   used predefine hostnames WN
3. The CA runs the update script with the new cslan-4.5.5.tar.gz file:

   ```
   update.sh /home/cslagent/cslan-4.5.5.tar.gz
   ```
4. The CA checks which partition is booted using the getBoot.sh tool

   ```
   getBoot.sh
   ```

   This will return either 1 or 2. The previous command will have updated the inactive partition.

   used alternative ssh command WN
5. The CAs the boot partition you just updated to be started after reboot:

   ```
   setBoot.sh usern
   ```

   (where n is the partition number of the inactive partition)

   ssh cslagent@subs
6. The CA reboots the CryptoServer LAN into the inactive partion

   reboot

WN 23:33

The CA updates the operating system in the second boot partition

1. **The CA checks that the inactive partition has the expected version:**

   ```
   csadm Dev=192.168.4.204 CSLGetVersion
   ```

   Expect 4.5.5

   used predefine hostname WN
2. The CA logs into the CryptoServer LAN as the cslagent user via SSH

   ```
   ssh 192.168.4.204 -l cslagent
   su -l
   ```
   (the CA supplies the default cslagent password)

   used alternative ssh command WN
3. The CA runs the update script with the new cslan-4.5.5.tar.gz file:
   update.sh /home/cslagent/cslan-4.5.5.tar.gz
4. The CA checks which partition is booted using the getBoot.sh tool

   ```
   getBoot.sh
   ```

   This will return either 1 or 2. The previous command will have updated the inactive partition.
5. The CAs the boot partition you just updated to be started after reboot:

   ```
   setBoot.sh usern
   ```

   (where n is the partition number of the inactive partition)
6. The CA reboots the CryptoServer LAN into the inactive partion

   ```
   reboot
   ```
7. **The CA checks that the inactive partition has the expected version:**
   ```
   csadm Dev=192.168.4.204 CSLGetVersion
   ```

   Expect 4.5.5

0.21 **The CA lists CryptoServer Firmware Modules**

CA Commentary: "These are the Firmware modules loaded a part of the Crypto Server clear process"
./csadmn Dev=192.168.4.204 ListFirmware

Expect: Useel predefine hostname WN

ID name type version initialization level
---

0 SMOS C64 5.5.9.1 INIT_OK
4 POST C64 1.0.0.2 INIT_OK
a HCE C64 2.2.2.3 INIT_INACTIVE
d EXAR C64 2.2.1.1 INIT_INACTIVE
68 CXI C64 2.3.0.5 INIT_OK
81 VDES C64 1.0.9.3 INIT_OK
82 PP C64 1.3.1.7 INIT_OK
83 CMDS C64 3.6.2.0 INIT_OK
84 VRSA C64 1.3.6.1 INIT_OK
85 SC C64 1.2.0.3 INIT_OK
86 UTIL C64 3.0.5.1 INIT_OK
87 ADM C64 3.0.25.5 INIT_OK
88 DB C64 1.3.2.2 INIT_OK
89 HASH C64 1.0.11.2 INIT_OK
8b AES C64 1.4.1.4 INIT_OK
8d DSA C64 1.2.3.3 INIT_OK
8e LNA C64 1.2.4.2 INIT_OK
8f ECA C64 1.1.12.4 INIT_OK
91 ASN1 C64 1.0.3.6 INIT_OK
96 MBK C64 2.2.8.2 INIT_OK
9a NTP C64 1.2.0.9 INIT_OK
9c ECDSA C64 1.1.16.1 INIT_OK

WN 23:34

0.22 CA Commentary: "The subordinate HSM has now been purged and the CSLAN and firmware images have been updated to the latest versions"

WN 23:35

0.23 CA Commentary "The only existing user is the default admin"

The CA present the list of users
csadm Dev=192.168.4.204 ListUser
expect only default ADMIN user, if not re-purge

Useel predefine hostname WN

WN 23:35

Niewoźniczański

Both HSM powerdown 23:39

Niewoźniczański